POLITECNICO DI TORINO
Repository ISTITUZIONALE

e-Health: New Frontiers and Challenges for Healthcare

Original
e-Health: New Frontiers and Challenges for Healthcare / Molaschi, V.. - In: EUROPEAN REVIEW OF DIGITAL ADMINISTRATION & LAW. - ISSN 2724-5969. - 4:(2023), pp. 3-297. [10.53136/9791221811285 01]

Availability:
This version is available at: 11583/2994159 since: 2024-11-05T10:39:27Z

Publisher:
Aracne

Published
DOI:10.53136/9791221811285 01

Terms of use:

This article is made available under terms and conditions as specified in the corresponding bibliographic description in the repository

Publisher copyright

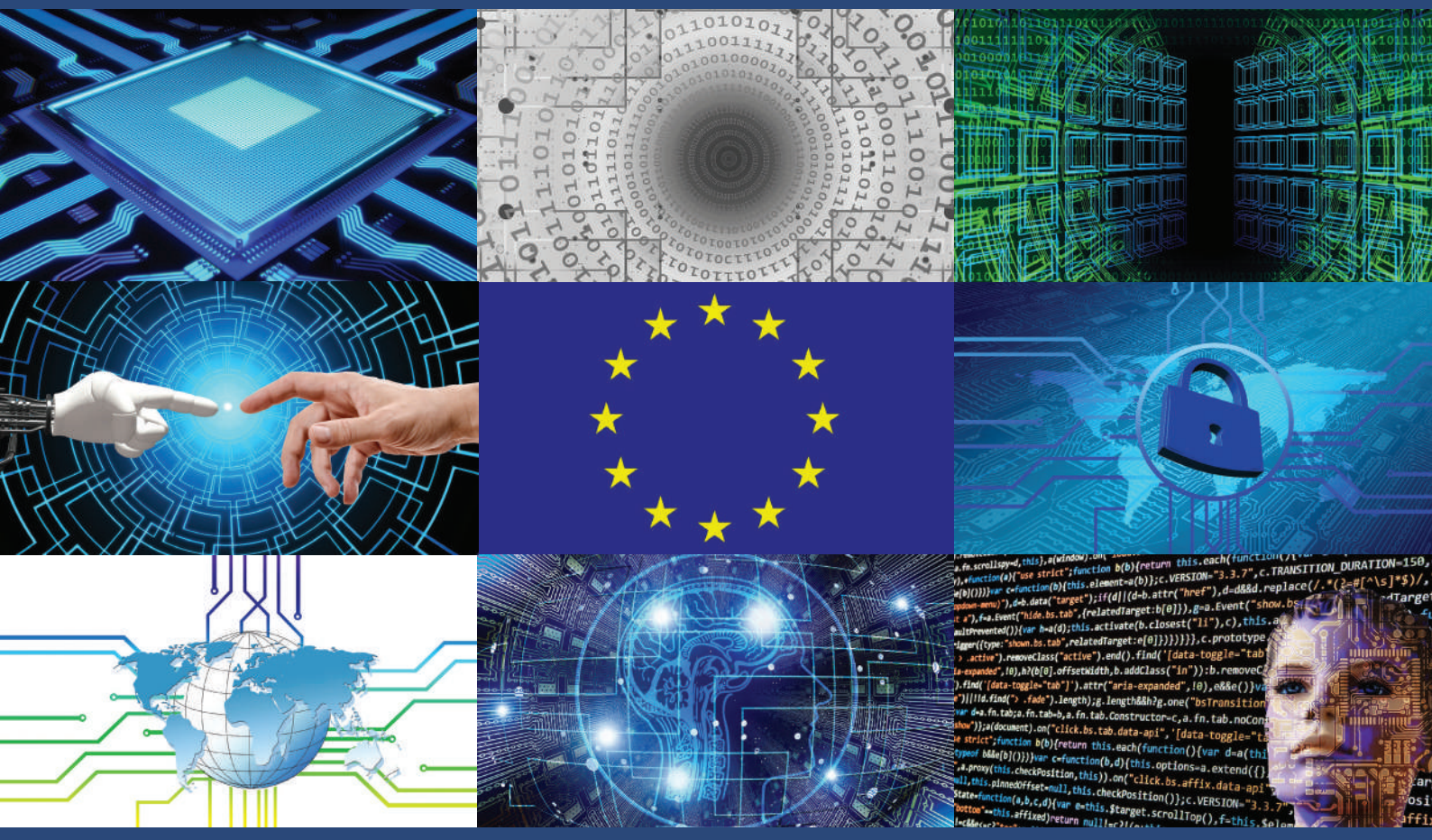
(Article begins on next page)

23 September 2026

EUROPEAN REVIEW OF DIGITAL ADMINISTRATION & LAW

VOLUME 4
ISSUE 1
2023

E-HEALTH: NEW FRONTIERS AND CHALLENGES FOR HEALTHCARE



aracne

ERDAL

European Review of Digital Administration & Law / Erdal – *biannual review*

Editors in chief
Angelo Giuseppe Orofino, Julián Valero Torrijos.

Associate editors
Ignacio Alamillo Domingo, Marcos Almeida Cerreda, Massimiliano Balloriani, Miguel Ángel Bernal Blay, Nadja Braun Binder, Fabio Bravo, Elena Buoso, Maciej Błażewski, Dolors Canals Ametller, Antonio Cassatella, Agustí Cerrillo i Martínez, Emilie Chevalier, Lucie Cluzel-Métayer, Fulvio Costantino, Zsolt Czékmann, Elise Degrave, Silvia Diez Sastre, Dacian C. Dragos, Lena Enqvist, Manuel Fernández Salmerón, Francesco Follieri, Isabel Celeste Fonseca, Cristina Fraenkel-Haeberle, Isabel Gallego Córcoles, Giovanni Gallone, Caroline Lequesne Roth, Daniele Marongiu, Isaac Martín Delgado, Rubén Martínez Gutiérrez, Ricard Martínez Martínez, Anne Meuwese, Viviana Molaschi, Hanne Marie Motzfeldt, Katrin Nyman-Metcalf, Catherine Prébissy-Schnall, Timo Rademacher, Sofia Ranchordas, Catarina Sarmento e Castro, Stefano Salvatore Scoca, Markku Suksi, Maria Supera-Markowska, Joe Tomlinson, Clara Isabel Velasco Rico.

Scientific committee
Jean-Bernard Auby, Antonio Barone, Eloísa Carbonell Porras, Enrico Carloni, Maria Cristina Cavallaro Vincenzo Cerulli Irelli, Jacques Chevallier, Stefano Civitarese Matteucci, Guido Corso, Philippe Cossalter, Lorenzo Cotino Hueso, Paul Craig, Patrizia De Pasquale, Domenico D'Orsogna, Marco Dugato, Giovanni Duni, Vera Fanti, Enrico Follieri, Fabrizio Fracchia, Fabio Francario, Diana-Urania Galetta, Eduardo Gamero Casado, Solange Ghernaouti, Jacek Gołaczyński, Annette Guckelberger, Gilles J. Guglielmi, Martin Ibler, Marc Jaeger, Ann-Katrin Kaufhold, Christine Leitner, António Cândido Macedo de Oliveira, Francesco Manganaro, Roberto Martino, Monica Palmirani, Andrea Panzarola, Nino Paolantonio, Hélène Pauliat, Sergio Perongini, José Luis Piñar Mañas, Ferdinando Pinto, Giuseppe Piperata, Aristide Police, Pier Luigi Portaluri, Yves Poullet, Gabriella Margherita Racca, Olivier Renaudie, Mauro Renna, Maria Alessandra Sandulli, Giovanni Sartor, Stephanie Schiedermair, Franco Gaetano Scoca, Karl-Peter Sommermann, Fabrizio Tigano, Luisa Torchia, Piera Maria Vipiana.

Editorial board
Beatriz Agra Costa, Simona Attolino, Marie Bastian, Amélie Bellezza, Antonio David Berning Prieto, Noelia Betetos Agrelo, Vinicio Brigante, Carla Casanueva Muruáis, Léonore Cellier, Juan Ignacio Cerdá Meseguer, Anna Maria Chiariello, Andrea Circolo, Angela Correra, Pedro Cruz e Silva, Gustavo Manuel Díaz González, Viviana Di Capua, Alessandro Di Martino, Luna Felici, Emanuele Grippaudo, C. Elio Guarnaccia, Mehdi Kimri, Maximilien Lanna, Gerard Loïck, Marco Mancarella, Elisabetta Marino, Michele Martoni, Manfredi Matassa, Javier Miranzo Díaz, Marco Mongelli, Julien Mongrolle, Julie Mont, Raphaël Mourère, Bernardo David Olivares Olivares, Alessia Palladino, Luís Manuel Pica, Alessandro Pisani, Luigi Previti, Quentin Ricordel, Luigi Rufo, Alfonso Sánchez García, Nadia Ariadna Sava, Felix Schubert, Balázs Szabó, Guillaume Tourres, Sabrina Tranquilli, Sara Trota Santos.

Submitting manuscripts
Manuscripts should be submitted via email to info@erdalreview.eu
For any queries on submission guidelines and procedures, please contact the Review.

Citation format
Editorial rules can be downloaded from the Review website.

Peer review procedure
This journal uses a double-blind review model.

Subscriptions
For subscriptions please contact: info@adiuvaresrl.it

Creative Commons License (CC BY-NC-ND 4.0) creativecommons.org/licenses/by-nc-nd/4.0/
You are free to share, copy and redistribute the material with correct attribution, you may not use the material for commercial purposes and you may not modify or transform it

Responsible Director: Angelo Giuseppe Orofino. Review registered at no. 12 of press register of the Court of Bari on 15 July 2020.

European Review of Digital Administration & Law

2023 Volume 4
Issue 1

ERDAL

This issue has been supported by three research projects:

"Patient empowerment, health data space and artificial intelligence as the basis of the new healthcare system" (22041/PI/22).
It is funded by the Seneca Foundation, Science and Technology Agency of the Region of Murcia, Spain.





PRIN (acronym for "Projects of Significant National Interest") called "Artificial Administrative Intelligence for territorial equality" (2022KLAJ4P).







Project "Ciudadanía administrativa digital y su reflejo administrativo/Digital Citizenship and its Administrative Reflection (CIADIG)", TED2021-129283B-I00, financiado por MICIU/AEI /10.13039/501100011033 y por la Unión Europea NextGenerationEU/ PRTR





©

ISBN
979-12-218-1128-5

I^ST EDITION
ROMA 30 SEPTEMBER 2023

TABLE OF CONTENTS

Monographic Section: *e-Health: New Frontiers and Challenges for Healthcare*

(eds. María Belén Andreu Martínez, Viviana Molaschi and Olivier Renaudie)

EDITORIAL

María Belén Andreu Martínez, Viviana Molaschi and Olivier Renaudie, *e-Health: Opportunities and Critical Issues for the Patient and for Health Services* ..... pag. 5

DIMENSIONS, FIELDS AND APPLICATION ISSUES OF E-HEALTH

Elena di Carpegna Brivio, *e-Health as a Multilevel Public Policy* ..... » 7

Nieves de la Serna Bilbao and Fernando Fonseca Ferrandis, *European Data Strategy. An Approach to the European Health Data Space. The Role of the Regulation (Eu) 2022/868 of the European Parliament and of the Council of May 30, 2022 Relating to European Data Governance* ..... » 17

José Vida Fernández, *Regulation of Artificial Intelligence in Healthcare within the European Union* ..... » 33

Paulina Gruszka and Małgorzata Kozłowska, *e-Transformation in the Polish Healthcare System. Data in Healthcare Entities* ..... » 49

Juan José Mantilla Sandoval, *Liability of the Spanish Health Administration for the Use of Artificial Intelligence* ..... » 57

Miklós Zorkóczy, *HealthTech and AI in Hungary* ..... » 71

María Estrella Gutiérrez David and José Luis Quintana Cortés, *Public Procurement of AI for the EU Healthcare Systems. First Insights from the Spanish Experience* ..... » 87

Carlo Casonato, *Tele-doctors? Navigating the Future of Healthcare: Advantages and Risks of AI-Enhanced Telemedicine* ..... » 141

Olivier Renaudie, *Telehealth: A New Relationship with the Territory(ies)?* ..... » 147

Viviana Molaschi, *Telemedicine: Impact and Perspectives in Healthcare Delivery and Organization of the Italian National Health Service* ..... » 153

Gabriella Berki, Gergely Toth and Zsolt Czékmann, *The Development of Telemedicine and its Application Possibilities in Hungary* ..... » 169

Andrea Salud Casanova Asencio and María Belén Andreu Martínez, *Primary Use of Data in the European Health Data Space Proposal: Its Impact on National Electronic Health Records from a Spanish Perspective* ..... » 177

Nicola Posteraro and Stefano Corso, *The Italian Electronic Health Record*

(EHR) » 187

Giulia Caldera, *Digital Therapeutics: An Ongoing Revolution* » 201

Maurizio Campagna, *Public and Private Participation in Digitalised Healthcare* » 211

Simone von Hardenberg and Lauren Tonti, *Digital Demands: An Overview of the Journey Toward Access and Reimbursement in the German Statutory Health Insurance* » 221

Balázs Szabó, *e-Health Care in Hungary With the Help of Ict Tools* » 233

Maciej Błażewski and Michał Raduła, *System of e-Heath tools. The Example of Poland* » 243

Neville Harris, *Health and Disablement Among Social Security Recipients in the UK: The Role of Digital Communication and Capacity in Assessments and Entitlements* » 249

e-Health and Cybersecurity

Marcel Moritz, *The Cybersecurity of Health Data Hosted by Public Administrations* » 267

Carlos Galán Cordero, *Cybersecurity of Information Systems in the Public Healthcare* » 273

Francesco Saverio Romolo, Simone Grassi, Alessandro Di Luca, Michela Previtali and Antonio Oliva, *Health and Cybercrime* » 287

Studia Varia

Rocío Navarro González, *Artificial Intelligence as a Strategic Opportunity to Rearrange and Renew Public Management* » 299

Case Analysis

Alessandro Di Martino, *More on Algorithms and Public Administration* » 307

Book Review

Giovanni Gallone, *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo*, Cedam, Milan, 2023, reviewed by Michele Trimarchi » 313

Eva Menéndez Sebastián, *From Bureaucracy to Artificial Intelligence. The Tension Between Effectiveness and Guarantees*, Cedam, Milan, 2023, reviewed by Giulia G. Cusenza » 320

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 5-6
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 01

e-Health: Opportunities and Critical Issues for the Patient and for Health Services

María Belén Andreu Martínez, Viviana Molaschi and Olivier Renaudie

By digital health (e-Health) is meant as all the tools and services that use information and communication technologies (ICTs) to improve prevention, diagnosis, treatment, monitoring and management of health-related issues and to monitor and manage lifestyle-habits that impact health. The evolution toward increasingly digitized health and health care represents a revolution in the way health is protected and health services are delivered.

To give an idea of this heterogeneous and growing set of instruments, one, aware that they are undergoing continuous transformation, can only take a descriptive approach and formulate a few of the most significant examples.

Telemedicine, which consists of remote diagnosis, treatment and monitoring of patients, is the first manifestation of the digital health phenomenon, its original and still current pillar.

Digital health, however, has expanded to other areas of medicine and healthcare.

One of the most forward-looking frontiers are digital therapies or "digiceuticals", that are therapeutic interventions whose "active substance" is a software, a digital tool.

Also not to be forgotten are the contribution to medicine and healthcare of algorithms, which are becoming increasingly advanced through machine learning and artificial intelligence techniques. Algorithms intercept the phenomenon of "big data", that incredible amount of digital information, characterized by unprecedented volume, speed and variety, which is the chosen terrain for their operation. Algorithms have computational and predictive capabilities unimaginable to a human.

Algorithms can analyse radiological images and provide diagnoses very quickly; they can also make accurate predictions about the course of diseases.

Looking at current events, the use of algorithms has proved crucial in the fight against the Covid-19 pandemic.

Artificial intelligence and big data are the most important allies of precision medicine, an emerging approach to treating and preventing disease, which takes into account genetic, environmental, and lifestyle variability in the individual patient.[1] Precision medicine enables therapies tailored for each individual and therefore more appropriate, effective and efficient, while containing the risk of adverse or undesirable events.

Digital health also consists of a range of tools aimed at improving health services, in particular by simplifying the relationship between healthcare facilities, professionals and citizens.

Let us think of the electronic health record, the "digital health identity card of the individual citizen"[2] and of the other examples of dematerialization in healthcare, like the electronic medical record or e-prescription. Part of digital health care are also electronic reservation systems for access to health care services, which are helpful in reducing waiting times.

In addition, the important role of health data in many of these tools should not be forgotten and will be further enhanced (for both primary and secondary uses) by the European Health Data Space.

In this issue of Erdal, we aim to represent the phenomenon of digital health with as broad and inclusive a view as possible, giving space to its various manifestations and showing the variety and pervasiveness of the phenomenon.

Sometimes e-Health tools will be the subject of a devoted reflection, dropped into the specifics of a national reality, as in the case of articles on telemedicine, on the electronic health records or on digital therapies. Sometimes an overview of the main e-Health instruments will be provided, especially in those papers that provide a

[1] See the definition given by the U.S. Food and Drug administration: www.fda.gov/medical-devices/in-vitro-diagnostics/precision-medicine.

[2] In these terms see G. Polifrone, *Sanità digitale. Prospettive e criticità di una rivoluzione necessaria*, Milan, Lswr, 2019, 11.

general picture of the development of digital health in particular countries.

The essays that make up this issue are intended to stimulate a balanced analysis on the different sides of the application of ICTs to health care, highlighting advantages and criticalities, potentials and uncertainties, in order to avoid the risk of incurring techno-optimism or techno-pessimism.

The reflections unfold on two planes: both the impact of digital health on the role played by the sick person with respect to his or her own health and course of care, an issue that also involves the doctor-patient relationship, and the impact on welfare systems.

Regarding the first aspect, e-Health is certainly an exceptional tool for patient empowerment.

The concept of empowerment takes on a significant declination in health care where patient empowerment is defined as the "process of personal development whereby the patient/individual is endowed with knowledge, skills and awareness that enable him/her (in whole or in part) to self-determine in relation to his/her own health".[3]

First and foremost, e-Health creates the preconditions for such empowerment: in fact, it opens up unbelievable possibilities for access to health care services.

Secondly, it seeks to provide answers to instances that are increasingly becoming part of the demand for health services: the need for direct and immediate health information; the request for direct management of one's own data and the various diagnostic and therapeutic options available, which allows greater control on one's own health; the demand for a more direct and informal, as well as faster relationship with health professionals or, more in general, with health facilities.

However, there are also problematic aspects. Let us think of the risks related to privacy, data quality and security of a data-driven medicine and healthcare, issues that regard both the individual and the digital health system as a whole. Some scholars have also underlined the issue of patient self-vulnerability that may result from the availability of personal clinical data even without the mediation of the physician.[4] This issue can be made even more serious because nowadays people can freely turn to the web for medical or supposed medical services and for buying drugs without the guide of an expert physician.

Another critical matter is the de-humanization of the physician-patient relationship, that can be iconically expressed through the image of the "robot-doctor".[5]

Moreover, one cannot forget the possible discrimination arising from the digital divide, due to which access to and informed use of tools are conditioned by factors such as age, socio-economic status, etc.

The analysis of the impact of digital health on welfare systems moves from the consideration that digital health does not only pertain to the field of health care delivery, but also encompasses political-administrative processes that relate to e-Health.[6]

In the various articles of this issue the topic is always approached from a multilevel perspective, aimed at investigating the influence of the European Union, despite the absence of specific competencies on health, and delving into the situation at the national and sub-national levels.

E-Health is an engine for modernization and greater efficiency of health systems, which can make a significant contribution in addressing what is now the key problem of health services in different countries: sustainability.

However, we will see that the development of digital health is characterized by numerous implementation problems and proceeds in "variable geometry" with significant differences between countries and between areas within the same country. Often the performance and organizational problems that plague health services, affecting the patients' health, are "reproduced" in the difficulties and delays in developing digital systems.

[3] On the impact of digital health on patient empowerment see E. Bellio, L. Buccoliero and A. Prenestini, *Patient web empowerment: la web strategy delle aziende sanitarie del SSN*, in *E. Cantù* (ed.), *L'aziendalizzazione della sanità in Italia: rapporto Oasi 2009*, Milan, EGEA, 2009, 413 et seq.

[4] See A. Pioggia, *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in R. Cavallo Perin (ed.), *L'amministrazione pubblica con i big data: da Torino un dibattito sull'intelligenza artificiale*, Rubbettino Editore, Soveria Mannelli (CZ), 2021, 222.

[5] See R. Balduzzi, *Cinque cose da fare (e da non fare) in sanità nella (lunga e faticosa) transizione verso il post-pandemia*, in *Corti supreme e salute*, 2020, 353.

[6] For this observation see N. Matteucci and N. Marcatili, *E-health ed evoluzione dei sistemi sanitari. Un'analisi empirica sull'Europa*, in G. Vicarelli e M. Bronzini (eds.), *Sanità digitale. Riflessioni teoriche ed esperienze applicative*, Bologna, il Mulino, 2019, 51.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 7-16
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 02

*e-Health as a Multilevel Public Policy**

Elena di Carpegna Brivio
(Assistant Professor of Public Law at University of Milan-Bicocca)

ABSTRACT. The pandemic has highlighted how public organizations must increasingly abandon the logic of rigid attributions of competence to embrace instead the effective pursuit of public policies. In this regard, e-Health represents a particularly significant case, because it sees specific goals set by the European Union be implemented by Regions and Municipalities, while the State assumes the role of facilitator and coordinator.

1. *A new season for Public Law*

1.1. *Less separation of competencies, more public policies*

The Coronavirus pandemic has radically changed the development of public policies. The emergency has exposed an institutional framework that, previously, was difficult to perceive beneath the legislative model. While social distancing was depriving society of all the connections that spontaneously animate the development of a community, it became clear how unrealistic it was to think of public action starting from abstract lists of competencies. Instead, it emerged how necessary it is to set service goals and then go looking for the institutional actors that could rebuilt the post-pandemic world on a solid foundation.

Legal scholars witnessed the first phase of the emergency, emphasizing how much the grounding concepts of their discipline struggled to adapt to the fast-moving new reality. Today, however, it is evident how the emergency has opened up a new phase that could permanently influence how political institutions deal with the problems of their communities. In particular, it is now evident the importance of crossing all the institutional and territorial separation of competencies to effectively care for the new needs of the population.

This essay aims to highlight how the driving force behind this transformation has been the European Union, which has addressed the pandemic emergency by defining a series of new goals that, to be realized, require a substantial enhancement of territorial systems, with regions and municipalities acting as the public entities that can nuance the unitary purposes according to the territorial needs.[1]

The old concept of territorial institutions that defend their particularism is then replaced by a vision that conceives equality in rights and services as the result of careful calibration of public interventions.[2]

The role of the States, in this context, is no longer to act as a central decision-maker but to become a facilitator and coordinator of the various actions needed in the territories.

This essay aims to verify how this happened, analysing a specific public policy, e-Health, that lies at the heart of the post-pandemic social reconstruction. Indeed, this is an area where the transformation of public policies can be very well verified. Although the European legal competence in health is minimal, e-Health is a key element for the post-pandemic EU agenda.[3]

The paper is organized into three sections. In the first one, paragraph 1.2 traces the emerging model, with a focus on how the EU has been able to use its competencies to build new paths of cooperation with Member States and sub-national institutions. Then, in the second section, paragraphs 2.1 and 2.2 examine the rise of e-Health as a public policy around which innovative service goals have been set. It is highlighted how their implementation requires intense cooperation,

* Article submitted to double-blind peer review.

[1] S. Bekker, *The EU's Recovery and Resilience Facility: A Next Phase in the Socioeconomic Governance?*, in *Politics and Governance*, vol. 9, no. 3, 2021, 175; C. Buzzacchi, *Local governance: analisi dell'impatto del Recovery Fund sul rapporto di sussidiarietà tra Stato e Regioni e sull'organizzazione degli enti locali*, in G. Dolso (ed.), *Governare la ripresa. La Pubblica Amministrazione alla prova del Recovery Plan*, Trieste, Edizioni dell'Università di Trieste, 2022, 53.

[2] Such a perspective on autonomy had been particularly explored by some thinkers of the 1940s and had a strong influence on some constituent experiences after World War II. S. Trentin, *Stato-Nazione-Federalismo*, Milan, La Fiaccola, 1940; A. Olivetti, *L'ordine politico delle comunità*, Ivrea (Switzerland), Nuove Edizioni Ivrea, 1945; Ch. Eisemann, *La centralisation et la décentralisation: principes d'une théorie juridique*, in *Revue du droit public*, no. 1, 1947, 27.

[3] M. Guy, *Towards a European Health Union: What Role for Member States?*, in *European Journal of Risk Regulation*, vol. 11, no. 4, 2020, 757.

producing a new convergence between levels and territories. Paragraph 2.1 analyses in depth the method of building new European public policies. Starting with financial instruments such as EU4Health and the Recovery and Resilience Facility (RRF), the EU has developed the ambition to overcome, through the enhancement of e-Health, the traditional fragmentation of health services in the Member States. As a result, paragraph 2.2 then explores how the National Recovery and Resilience Plans (NRRPs) have articulated European e-Health goals into investment and reform projects. In particular, Italy's National Recovery and Resilience Plan (PNRR) is considered a critical case study. In Italy, competencies in health and care have, since the 1990s, been intensely fragmented amongst the central level of government, the Regions, and the Municipalities. The achievement of the Next Generation EU (NGEU) goals on e-Health is thus a significant test for the ability of post-pandemic strategies to overcome the fragmentations that traditionally affect the territorial management of social and health services.

Paragraph 3, as a third section, highlights, in the end, how this season of public law is an opportunity to realize, in a multi-stakeholder and multilevel approach, a new European substantive equality firmly rooted in social rights.

1.2. *A next generation of public policies*

The European Union hasn't replicated the legitimation mechanisms typical of Member States. Instead, it has built its political role on the identification of policy goals that, to be effectively achieved, require participation, technical surveys, negotiation with stakeholders, and monitoring activities.[4]

In this perspective, the EU competencies defined by the Treaties aren't elements of separation but norms enabling a pathway that breaks the correspondence between input and output to introduce, instead, the evaluation of outcomes as main criterion for consolidating the European integration.[5]

The primary tools for the implementation of this different way of policy making are the economic-financial powers of the Union: starting with the Maastricht Treaty, and even more following the Eurozone crisis, financial surveillance allowed Europe to assess in-depth and ex-ante the policies that Member States intend to pursue.[6]

The Pandemic, on the one hand, has significantly mitigated fiscal parameters. The decision, in March 2020, to use the general escape clause introduced with the Six Pack in the Stability and Growth Pact, allowed Member States to temporarily deviate from the path to the medium-term target to deal with the severe economic recession.[7] But, on the other hand, it has also opened up a new evolutionary phase in the integration process, less focused on compliance with quantitative parameters and more oriented explicitly to the definition of a new political vision.[8] This kind of change is particularly relevant. If, in the logic of the Rome Treaty, the European unification was conceived as a matter of great guiding principles and general policies, since the Maastricht Treaty, instead, being part of the European-integration process has been understood primarily as the ability to produce non-inflationary growth, to ensure an open-market economy with free competition, and to maintain balanced public finances.[9]

Following the Covid-19 crisis, European policies have not discarded the idea that the European process has a defining moment in economic-financial integration. Still, it has emerged the need to new overarching issues that should overcome the singularity

[4] U. Puetter and S. Fabbrini, *Catalysts of integration – the role of core intergovernmental forums in EU politics*, in *Journal of European Integration*, vol. 38, no. 5, 2016, 633.

[5] F.W. Scharpf, *Governing in Europe: Effective and Democratic?*, Oxford, Oxford University Press, 1999; A. von Bogdandy and J. Bast, *I poteri dell'Unione: una questione di competenza. L'ordine verticale delle competenze e proposte per la sua riforma*, in *Rivista italiana di diritto pubblico comunitario*, no. 2-3, 2002, 303; P.S.M. Leino-Sandberg, *The Institutional Politics of Ojective Choice: Competence as a Framework for Argumentation*, in S. Garben, I. Govaere (eds.), *The Division of Competences between the EU and the Member States: Reflections on the Past, the Present and the Future*, Oxford-Portland, Hart Publishing, 2017, 210.

[6] V.A. Schmidt, *Europe's Crisis of Legitimacy: Governing by Rules and Ruling by Numbers in the Eurozone*, Oxford, Oxford University Press, 2020.

[7] European Commission, *Communication from the Commission to the Council on the activation of the general escape clause of the Stability and Growth Pact*, COM (2020), 123 final.

[8] P. Genschel and M. Jachtenfuchs, *Postfunctionalism reversed: solidarity and rebordering during the COVID-19 pandemic*, in *Journal of European Public Policy*, vol. 28, no. 3, 2021, 350.

[9] G. Guarino, *Pubblico e privato nell'economia. La sovranità tra Costituzione e istituzioni comunitarie*, in *La Costituzione economica*, Padova, Cedam, 1997, 46.

perspective and definitely overcome the crises of the past decade.[10] In particular, the priorities set by the Commission with the European Green Deal and the digital single-market Agenda have been chosen as new guiding policies for a greener, more digital, and resilient post-pandemic Europe.[11]

The initial European responses to the COVID-19 crisis were financial instruments specifically targeted at overcoming the economic shock of the Pandemic. During the spring of 2020 the European Central Bank activated the Pandemic emergency purchase program (PEPP),[12] while the Commission and the Council defined a new European-Stability Mechanism loan and a new financing program called SURE to support the employment policies of the Member States.[13]

At the end of May 2020, however, the European strategy was already shaped into a holistic recovery plan, the Next Generation EU (NGEU).

The main characteristic of the NGEU is to be a large pot of resources (about 750 billion euros) made available to Member States under the specific condition of matching targets that can either consist of the implementation of structural reforms or the design and implementation of modern and innovative services.

With this in mind, the Next Generation EU is articulated in three components:

- the European Union Recovery Instrument (EURI) that distributes the resources across the different spending programs;
- the EU funds (mainly the Recovery and Resilience Facility, RRF, that covers 90 percent of the entire NGEU) that form the legal basis for spending in the single programs;
- an amendment to the Own Resources Decision that allows to raise the 750 billion euros through EU loans on the financial markets.[14]

The NGEU has turned around the financial flow to the territories and it also introduced a new method of investment in which reforms and services are not simply an outcome but are steps whose achievement determines the possibility of receiving additional resources.[15]

Consequently, negotiations between the EU and the Member States did not only focus on the financial amounts but also engage a wide confrontation on the new goals of the European integration.[16] Significantly, Member States were suddenly able to invest in their economies without incurring further debt and they could set a new relationship with their own multilevel public organization. While the single State has been responsible for defining its own Plan, the need to achieve specific outcomes has opened the opportunity to a new confrontation between the State and the local authorities responsible for bringing the new services to citizens and communities.

It is a relevant change in respect to the past decade. During the economic crisis, European financial targets were defined as quantitative restrictions. States were responsible for the aggregate of public finance and the single State could be inclined to bind the autonomy of territories to comply with the set parameters.[17]

[10] J. White, *Politics of Last Resort*, Oxford, Oxford University Press, 2020; P. Dermine, *The EU's Response to COVID-19 Crisis and the Trajectory of Fiscal Integration in Europe – Between Continuity and Rupture*, in *Legal Issues of Economic Integration*, vol. 47, no. 4, 2020, 337.

[11] Commission Communication, *The EU budget powering the recovery plan for Europe*, COM (2020) 442, 27 May 2020; Commission Communication, *Europe's moment: Repair and prepare for the Next Generation*, COM(2020)456, 27 May 2020.

[12] The PEPP is a non-standard monetary policy tool consisting of a temporary asset purchase program of private and public-sector securities: European Central Bank, Decision 2020/440, 24 March 2020.

[13] The SURE program (The temporary Support to mitigate Unemployment Risks in an Emergency) has been financed by the European Commission through the emission of social bond. With the last payment in December 2022, the Union provided 98.4 billion euros to all 19 member countries that applied: European Union Council, Regulation 2020/672, 19 May 2020.

[14] The NGUE was presented by the European Commission on 28th May 2020 and became effective in February 2021. For an analysis of its internal articulation B. De Witte, *The European Union's Covid-19 Recovery Plan: the Legal Engineering of an Economic Policy Shift*, in *Common Market Law Review*, vol. 58, 2021, 635.

[15] G. Falcon, *Viaggio al centro del PNRR*, in *Le Regioni*, no. 4, 2021, 715.

[16] P. Leino-Sandberg and M. Ruffert, *Next Generation EU end its Constitutional Ramifications: a critical Assessment*, in *Common Market Law Review*, vol. 59, 2022, 433; N. Lupo, *Next Generation EU e sviluppi costituzionali dell'integrazione europea: verso un nuovo metodo di governo*, in *Diritto pubblico*, no. 3, 2022, 729; B. De Witte, *The European Union*, 678.

[17] L. Schramm and W. Wessels, *The European Council as a crisis manager and fusion driver: assessing the EU's fiscal response to the COVID-19 pandemic*, in *Journal of European Integration*, vol. 45, no. 2, 2023, 257; J. Creel, N. Leron, X. Ragot and F. Saraceno, *Embedding the Recovery and Resilience Facility into the European Semester*, *ETUI Policy Brief*, no. 14, 2021; S. Bekker, *The social dimension of EU economic governance after the Covid-19 pandemic: exploring new inter-*

Now, the NGEU pushes the States to cooperate with their local authorities because achievements will be measured on the implementation of specific services and reforms.[18]

As a result, the State is no longer simply at the top of a closed system. It becomes, instead, a pivot point responsible for connecting the territories with the large-scale purposes defined at the European level.[19]

Specifically, the NGEU requires national-spending policies to align with two macro-policies outlined by the Union, the Green Deal and the Digital Agenda. They are the main guidelines around which the National Recovery and Resilience Plans (NRRPs) have been built.[20]

In order to build their own National Plans, the States were thus nudged to explore the potential of their domestic system and then to design a development strategy that could match with that.[21]

This approach required a new effort for States because to be compliant with Union law they have to develop a new method of governance that should verify the achievement of objectives, solve any problems of implementation, and be accountable according to a logic of coordination and support of their territories.[22]

2. *The e-Health and the question of multilevel governance*

2.1. *The European policies of e-Health after the Pandemic*

One of the main effects of the COVID-19 Pandemic has been to radically change the impact of technology and digitization on daily life.

Healthcare was undoubtedly one of the areas that had to rethink its functioning to cope directly with the emergency and to reorganize all other healthcare services that, with social distancing, could no longer run normally. In particular, prevention and monitoring suffered severe delays and rescheduling with a significant impact on diagnosis and daily care.

In addition, the widespread acceleration of remote activities made it clear how, in the health-care field, Telemedicine could open up potentials hitherto only partially explored. Remote technologies revealed also new relationships between healthcare and assisted living that, in perspective, could become pivotal assets for welfare systems facing the aging of populations.[23]

In the European Union, the pandemic discussion on ICT became part of the path towards e-Health that the Union had launched before the Covid emergency. E-Health is meant as the use of information and communication technologies for improving patient health and increasing the efficiency of the healthcare system as a whole. European policies on e-Health involved, before the Pandemic, the use of Telemedicine, the implementation of electronic records, and health-information exchange.[24]

linkages, in *Italian Labour Law e-Journal,* vol. 15, no. S1, 2022, 1.

[18] A. Biondi and O. Stefan, *EU Health Union and State Aid Policy: With Great(er) Power Comes Great Responsibility*, in *European Journal of Risk Regulation*, vol. 11, 2020, 894.

[19] The priorities and limitations within which the National Plans must move are set out at the EU level. In particular, the NGEU has indicated the need to converge spending policies with certain macro-policies indicated by the Union, the Green Deal and the Digital Agenda, which constitute the major guidelines around which the National Recovery and Resilience Plans (NRRPs) have been built. Regulation 2021/241. S. Bekker, *The EU's Recovery and Resilience Facility: A Next Phase in the Socioeconomic Governance?*, in *Politics and Governance*, vol. 9, no. 3, 2021, 175; N. Lupo, *Il Piano Nazionale di Ripresa e Resilienza: un nuovo procedimento euro-nazionale*, in *Federalismi.it*, 15 February 2023; G. Piccirilli, *Il PNRR come procedimento euro-nazionale e la "fisarmonica" governativa*, in V. Di Porto, F. Pammolli, A. Piana (eds.), *La fisarmonica parlamentare tra pandemia e PNRR*, Bologna, Il Mulino, 2022, 137.

[20] P. Leino-Sandberg and M. Ruffert, *Next Generation EU*, 455.

[21] L. Schramm, U. Krotz and B. De Witte, *Building Next Generation after the pandemic: The implementation and implications of the EUCovid Recovery*, in *Journal of Common Market Studies*, vol. 60, 2022, 114; S. Rainone, *From deregulatory pressure to laissez faire. The (moderate) social implications of the EU recovery strategy*, in *Italian Labour Law e-journal*, vol. 15, no. 1s, 2022, 30.

[22] Article 18(q) of the RRF requires the Member States to include regional and local authorities and other relevant stakeholders in the design and implementation of the policies contained in the NRRP. A specific section of the plan must then be devoted to the consultation of these stakeholders. S. Bekker, *The social dimension of EU economic governance after the Covid-19 pandemic*, 11.

[23] I. Ahmad, Z. Asghar, T. Kumar *et al*., E*merging Tchnologies for Next Generation Remote Health Care and Assisted Living*, in *IEEE Access*, vol. 10, no. 4, 2022, 1.

[24] M.M. Luca, L. Mustea *et al.*, *Challenges on Radical Health Redesign to Reconfigure the Level of e-Health Adoption in EU countries*, in *Frontiers in Public Health*, vol. 9, 2021, 1; S. Whitelaw *et al*., *Application s of digital technology in COVID-19 pandemic planning and response*, in *Lancet Digital Health*, no. 2, 2020, 435.

In 2008 the Commission's communication *Telemedicine for the benefit of patients, health systems and society* encouraged Member States to increase their telemedicine efforts.[25]

Then, in 2019, Recommendation n. 2019/243 signaled out digital health records as elements to be framed within the right to cross-border health care recognized in Directive n. 2011/24.[26] It was a relevant tool meant to create in the European area a health data-sharing environment and a homogeneous grounding for health services and care paths that could cover the whole territory of the Union.[27]

With the Pandemic, a regulatory framework capable of ensuring, at the European level, an effective and safe infrastructure for the management of patient health data became a priority. However, it also became clear how challenging it was for Europe to fit into a subject, Healthcare, where EU competencies are minimal and differences between Member States are very pronounced.[28]

Indeed, in this case, the element that enabled the European institutions to formulate an EU policy on e-Health was different from an actual title of competence. The establishment of the Multiannual Financial Framework for 2021-2027, in December 2020, provided the occasion for the development of a new European strategy on the subject.[29] The Framework designed two specific programs on digitization. The first, Digital Europe, aimed to govern a generalized transition to digital technologies focusing on artificial intelligence and cybersecurity. The second was called EU4Health and strengthened the Union's role in disease prevention and health protection. The program, funded with 5.1 billion Euros, explicitly aimed at fostering cooperation amongst national health systems. The countries should bring the digital health record fully operational, develop joint diagnostic studies and share the results of health-technology assessment processes through Health Technology Assessment (HTA).[30]

In addition, 20 percent of the fund has been reserved for disease promotion and prevention activities with a work program to strengthen health systems, improve access to health services and build a data infrastructure that should support Member States' health policies. EU4Health has also helped shape a broader initiative called the European Health Union (EHU), announced by President Ursula von der Leyen in September 2020 and involving a series of legislative proposals to strengthen the European role in health.[31]

With the definition of the Next Generation EU, the European healthcare role has been shaped through loans and grants subject to minimal conditionality.[32] It was a step forward towards a European integration based on solidarity between countries and on the ability of the Union's policies to reduce inequalities in the different territories. Moreover, the Recovery and Resilience Facility (RRF), NGEU's largest fund, has the double goal of mitigating the impact of the Pandemic and accelerating the transition to a green and digital economy. With this in mind, the Commission sought to guide the use of the

[25] European Commission, *Telemedicine for the benefit of patients, health systems and society*, COM (2008) 689, 4 November 2008.

[26] Commission Recommendation, *On a European Electronic Health Record exchange format*, no. 2019/243 of 6 February 2019. European Parliament and Council, directive no. 2011/24/EU *on the application of patients' rights in cross-border healthcare*, 9 March 2011.

[27] T. Ferreira, *E-Health Application and Data Protection: a comparison of selected European Union memebers' national legal systems*, in *Bioethica*, vol. 8, no. 1, 2022, 74.

[28] The Union's health competencies are defined by 168 TFEU, §§ 2, 5, 7. They primarily give the Union a role in supporting and complementing States' competencies in health field. K. Purnhagen, M. Flear *et al*., *More competences than you knew? The web of health competences for Union action in response to the COVID-19 outbreak*, in *European Journal of Risk Regulation*, vol. 11, no. 2, 2020, 297; E. Brooks, *European Union health policy after the pandemic: an opportunity to tackle health inequalities?*, in *Journal of Contemporary European Research*, vol. 18, no. 1, 2022, 67.

[29] Council of the EU, *Multiannual financial framework for 2021-2027*, 17 December 2020; Council Regulation (EU, Euratom) 2020/2093, Laying down the multiannual financial framework for the years 2021 to 2027, 17 December 2020.

[30] European Parliament and Council, Regulation On the establishment of a Program for the Union's action in the field of health –for the period 2021-2027and repealing Regulation (EU) No 282/2014 ("EU4Health Programme"), COM (2020) 405 final; European Commission, Annex to the Implementing Decision on the financing of the Programme for the Union's action in the field of health ('EU4Health Programme') and the adoption of the work programme for 2021, C (2021) 4793 final, 24 june 2021.

[31] M. Guy, *Towards a European Health Union: What Role for Member States?*, in *European Journal of Risk Regulation*, vol. 11, no. 4, 2020, 757.

[32] E. Brooks and R. Geyer, *The development of EU health policy and the COVID-19 pandemic: trends and implications*, in *Journal of European Integration*, vol. 42, no. 8, 2020, 1057.

funds by identifying seven focus areas: clean technology and renewables, energy efficiency, sustainable transport, broadband services, digitalization of public administration, data cloud and sustainable processor capacities, and education and training for digital skills. The Commission has also established that National Plans should serve these priorities, ensuring that at least 37 percent of budgeted spending will be allocated to climate investments and reforms and that no less than 20 percent will promote the digital transition. Finally, national-spending plans should demonstrate that they address the four priorities (environmental sustainability, productivity, fairness, and macroeconomic stability) outlined in the 2021 Annual Sustainable Growth Survey. Within these goals there is ample room for investment and reform in health.

All the NRRPs developed by Member States include actions specifically aimed at improving and modernizing the national health system with digitization and integration between health and social-welfare policies.[33] The digital transformation of healthcare consistently appears in the pillars of different national plans.[34]

The next paragraph analyzes the Italian National Recovery and Resilience Plan (PNRR) as a particularly significant case study for understanding how e-Health is changing the traditional logic of fragmented governance in healthcare.

2.2. *The impact of e-Health in the national health policies. The case of the Italian PNRR*

For Italy, health protection represents a key element of the welfare state designed by the 1948 Republican Constitution. Indeed, the Constitution expressly protects health (Art. 32) and several other social rights (Art. 33, 34, 35, 36, 37, 38). However, the structure of functions and competencies concerning social and health services has undergone a progressive devolution over the decades, with an increasing commitment of local governments to the realization of welfare goals.[35] In particular, since the 1990s, Regions and Municipalities have become essential providers of health and social-welfare policies. Regions are now responsible for organizing health services in the territory following standards established by the State to ensure minimum equality. At the same time, Municipalities are responsible for designing and delivering social-welfare services. A further element of complexity is that only the State finances the entire welfare. As a result, Italy presents an extremely differentiated organizational model with significant territorial variations in healthcare performance.[36] With dramatic evidence, the Covid-19 Pandemic has exposed how personal protection requires increasing complexity and interdependence and how it is necessary to implement policies to integrate services entrusted to separate authorities and administrations.[37]

The National Plan for Recovery and Resilience (PNRR) identifies the main issues affecting the Italian system and specifies how NGEU resources can help address them. There is a specific awareness of structural problems in the National Health System that the Pandemic has exacerbated. The Plan is articulated into six Missions (Digitization, Innovation, Competitiveness, Culture and Tourism; Green Revolution and Ecological Transition; Infrastructure for Sustainable Mobility; Education and Research; Inclusion and Cohesion; and Health) and every mission

[33] S. Bekker, *The social dimension of EU economic governance after the Covid-19 pandemic*, 3. For an analysis of the different RRPs see *Italian Labour Law e-Journal*, vol. 15, no. 1s, 2022.

[34] It is mainly the countries subjected to austerity during the financial crisis (Belgium, Italy, Portugal, Spain) that saw the NGEU as a vital opportunity to revive investment in social policies. In contrast, countries with greater fiscal capacity (Austria, Germany) built their National Plans around investments already planned. In this regard F. Corti, A. Liscai and T. Ruiz, *The Recovery and Resilience Facility: boosting investment in social infrastructure in Europe?*, in *Italian Labour Law e-Journal*, vol. 15, no. 1s/2022, 15.

[35] For an overview of the different reforms B. Pezzini, *Il riordino del 1992 (un sistema sanitario universale, nonostante il riordino del 1992)*, in *Corti supreme e salute*, no. 3, 2018, 559.

[36] For an anlysis over the different regional systems Vv. Aa., *L'integrazione socio-sanitaria e il diritto delle Regioni*, Rapporto 2022 dell'Osservatorio Diritto & Innovazione Pubblica Amministrazione Bicocca, Torino, Giappichelli, 2022; more in general S. Nicodemo, *Diritto dei servizi sociali*, Milano, Giuffré, 2021; A. Papa, *La tutela multilivello della salute nello spazio europeo. Opportunità o illusione?*, in *Federalismi.it*, no. speciale 4, 2018, 80.

[37] Italy was one of the countries most affected by the initial spread of the virus, with a particular impact on the most fragile population, such as the elderly. On the critical issues for the Italian system V. Molaschi, *Integrazione socio-sanitaria e COVID-19: alcuni spunti di riflessione*, in *Il Piemonte delle autonomie*, no. 2, 2020.

presents several different components.

Mission 6, funded with 15.63 billion euros, is integrally focused on healthcare. The Plan explicitly aims to effectively improve the National Health System into a more modern, digital, and inclusive service that will ensure equality equity of access by strengthening prevention and local services.[38]

Within Mission 6 there are two components: M6C1 (Neighborhood networks, facilities and telemedicine for territorial Healthcare) and M6C2 (Innovation, research and digitization of the national health service).

The first component aims to strengthen the services provided locally by creating territorial facilities and centers (such as Community Homes and Community Hospitals), investing in home care, developing Telemedicine, andfostering more effective integration amongst all social-health services.

Within the component, references to the digitization of healthcare are Reform 1 (Neighborhood networks, facilities, and Telemedicine for community healthcare and the National Health, Environment, and Climate Network) and Investment 1.2 (Home as the first place of care and Telemedicine). Achievement of Reform 1 will unlock further tranches of NGEU resources. Specifically, it involves the identification of a new healthcare strategy that should facilitate, through an overall reorganization and implementation of new performance standards, the approximation of the Italian Healthcare system to the best-performing European countries. This reform refers to Telemedicine only indirectly, as the Plan mainly refers to two distinct procedures that will define the new strategies. A ministerial decree should identify homogeneous structural, organizational, and technological standards for territorial care and the facilities assigned to it. The Government will present in Parliament also a proposal about the design of a new institutional integrated system for prevention following the One-Health approach that considers human health relying on institutional actions taken for the environment and climate.[39]

Regarding territorial facilities, the Plan identifies Community Homes as the place for coordinated services offered in the territory, particularly for chronic patients. Community Homes are the facilities where a multidisciplinary team of general practitioners, pediatricians, specialist physicians, nurses, and other social-service professionals should operate. In addition, the Community Home will be a permanent reference for the population, with the presence of the IT infrastructure, a point of withdrawal, multi-specialist instrumentations, and the Single Point of Access (PUA) for the multidisciplinary assessment of social-welfare needs.[40]

These purposes imply considerable coordination between Regions and Municipalities as they require an intense dialogue between health and social-welfare services. But it's investment 1.2 that raises even more strongly the question of territorial integration. The investment, called "Home as the First Place of Care and Telemedicine", contains a specific outcome target since it intends to upgrade healthcare home-based services for 10 percent of the population over 65 by 2026.[41]

Achievement of this goal involves four distinct actions:

- Identification of a shared model for home care that takes full advantage of the possibilities offered by new technologies (such as Telemedicine, home automation, and digitization);
- The implementation at each Local Health Authority (ASL) of an information system collecting clinical data in real time;
- The activation of 602 Territorial Operations Centers coordinating home care with other health services, ensuring a persistent dialogue with hospitals and the emergency network;
- The use of Telemedicine to better support patients with chronic diseases.[42]

The investment is financed with 4 billion euros; 1 billion is entirely dedicated to Telemedicine.

Particularly relevant is the provision that

[38] Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 225.

[39] The One-health approach is now recognized also by the European Commission and major international Health organizations. In this respect N. Posteraro, *La telemedicina*, in V. Bontempi (ed.), *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma, Roma Tre Press, 2022, 201.

[40] Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 228.

[41] Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 226.

[42] Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 228, 229.

the State should negotiate all the implementations related to the investment with the Regions and the Municipalities implicated in services.

Indeed, the identification of the home as the principal place of realization of social-welfare public policies implies a deep rethinking in the delivery of services because the institutions must coordinate, in a logic of mutual integration, to provide all the elements of care that can guarantee holistic social welfare. Thus, digitization takes on the role of fostering the full efficiency and interoperability of home-care services, and the Plan requires full coordination between the Mission on Healthcare and the actions for fragile population (e.g., elderly and people with disabilities) of other parts of the Plan.[43] For the purposes of this essay, it is then relevant that the PNRR plans to realize the investment by financing telemedicine projects proposed directly by the Regions and matching the priorities and guidelines set out by the Ministry of Health. Regional proposals can move along the entire care and treatment pathway, consisting of telecare, teleconsultation, telemonitoring, and telereport activities.

Projects will be funded only if they integrate with the Electronic Health Record (EHR), meeting precise quantitative targets and ensuring better health-service harmonization and the prioritization of multiregional projects.[44] The regional projects should be defined by the end of 2023, and the goal of the Plan is to assist through Telemedicine at least 200,000 people by 2025.

An additional aspect concerning the implementation of e-Health in the Italian PNRR is in the second component of Mission 6, M6C2, devoted to "Innovation, Research, and Digitization of the National Health Service."

In this component, funded by 8.63 billion euros, there are three targets:

- Development of the Healthcare strengthening investments in human, digital, structural, instrumental, and technological resources;
- Biomedical and health research;
- Digital innovation of the NHS, both at the central and regional level, in order to increase the quality, responsiveness, and involvement of patients.

7.36 billion is specifically intended for digitalizing hospitals with three separate actions: modernizing the hospital technology and digital stock, creating safe and sustainable hospitals, and strengthening the technology infrastructure for data collection, processing, analysis and simulation.[45] The latter action includes implementing the Electronic Health Record (EHR) and establishing a new technological infrastructure dedicated to data management at the Ministry of Health.[46]

The EHR is a central element of the digitization of healthcare as it is suitable for enhancing the delivery of digital health services and the value of national clinical data, fostering a new capacity for healthcare governance and planning. The main goal of the EHR is to promote accessibility, homogeneity, and harmonization of health services throughout the country. Although its introduction preceded the adoption of the PNRR, its pre-pandemic implementation proved only partially effective.[47] While all Italian Regions have introduced this tool, its use by caregivers varies significantly in different territories.[48]

The Pandemic has acted as a generalized wake-up call on the usefulness of digital tools. Still, their stable inclusion in Italian administrative culture requires the development of new policies.[49] Italy's PNRR is aware of this, and it intends to stimulate the use of EHR on the one hand by investing in the digital skills of individuals and, on the other hand, by allocating 0.74 billion euros for

[43] The investment should be coherent with investments 1.1 e 1.2, Component 2, Mission 5 (Social Infrastructure, Families, Communities and the Third Sector) dedicated to the support of vulnerable people, the prevention of institutionalization of the non-self-sufficient elderly, and pathways to autonomy for people with disabilities. Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 229.

[44] Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 229.

[45] A. Mascolo, *Lo Stato digitale nel PNRR – L'ammodernamento del sistema ospedaliero*, in *Osservatorio sullo Stato digitale IRPA*, 23rd of September 2021.

[46] Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 233.

[47] About EHR in Italy M. Ferrara, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *Federalismi.it*, no. 26, 2021.

[48] N. Posteraro, *La telemedicina*, 191.

[49] Istituto Superiore di Sanità, Report 12/2020; Conferenza permanente per i rapporti tra lo Stato, le Regioni e le Province autonome, *Indicazioni nazionali per l'erogazione di prestazioni in telemedicina.*

the training of health personnel.[50]

The Plan aims to make the EHR the access point for all essential services the National Health Service provides. It is also useful to create a homogeneous database able to adequately reconstruct patients' medical history and, on an aggregate basis, to predict future changes in the services. To this end, the Plan intends to unify all health records and bring them into a new central repository that must ensure uniform planning, management, and control tools in every territory, as well as full interoperability and data compatibility.[51]

In addition, the Ministry of Health will have to set up a new Health Information System (NSIS) as an infrastructure that should enable the central government to monitor compliance with basic levels of care and plan with a full knowledge of the changing needs on the ground.

To sum up, the Italian PNRR contains many ambitions for e-Health. On the one hand, there is a clear awareness of the need to focus on technological transformation to strengthen territorial medicine and improve the standards of care for citizens. On the other hand, telemedicine services are seen as an essential tool to address some structural problems of the National Health System and particularly to successfully address territorial gaps and enable new standards of care, especially in areas such as prevention.[52]

There is also awareness of how e-Health can create homogeneity in the use of services, significantly improving the care experience and fostering a multidisciplinary and flexible approach.

It is clear, however, that this approach requires a brand-new organizational culture because administrations can no longer consider their own set of competencies, functions and resources as separate property. The prescription within the PNRR of a series of collaborative and negotiated-planning tools is a step in the correct direction, as it is the introduction of coordinating bodies whose purpose is to guide the Plan implementation and resolve any critical issues. On October 11, 2021, the Interministerial Committee for Digital Transition formalized a working group on Telemedicine, and Agenas, the national agency for regional health services, formalized in September 2021 a technical working group on Telemedicine that should define standards for telemedicine services and draft guidelines for the implementation of a digital home care model.

In addition, according to the second report on implementation the government presented to Parliament on October 5, 2022, the Ministry of Health has signed institutional contracts with the Regions to develop Community Homes, Community Hospitals, and Home Care. It has also approved guidelines containing a digital model for implementing Home Care.

While these steps are undoubtedly positive, the actual realization of the goals will depend mainly on the adequacy of the administrative and technical structures of the subnational levels of government, which must formulate projects that are adequate to respond to the various lines of investment. Even before that, a key role will be played by the ability of the central government to direct, through the activation of public calls for proposals, the allocation of funds in a manner consistent with the objectives of the Plan.[53] So far, the entire ascending construction of the PNRR has been characterized by solid centralism. Modest has been the involvement of Regions and local authorities in goal setting, just as numerous are the instruments of control and substitution that leave the State with a strong influence in the entire implementation of the Plan.[54]

In conclusion, e-Health will be a serious test for Italy and it will allow to verify if Italian administrative culture has reached the necessary maturity to shape territorial relations through co-programming and co-designing.[55]

3. *Conclusions*

The Pandemic has highlighted how public policies cannot be effective through fragmentations and separations. It has downsized specific issues that, before, were central at the legal level. Today the lines

[50] Missione 6, *Formazione, ricerca scientifica e trasferimento tecnologico*, Componente 2 (M6C2), investimento 2.2, *Sviluppo delle competenze tecniche, professionali, digitali e manageriali del personale del sistema sanitario*.
[51] Italian Republic Government, *Piano nazionale di ripresa e resilienza*, 234.
[52] P. 22.
[53] C. Buzzacchi, *Local governance*, 54.
[54] On this matter European Committee of the Regions, *Regional and local authorities and the National Recovery and Resilience Plans*, 2021, 30.
[55] C. Buzzacchi, *Local governance*, 59.

between different institutional actors and levels of government are blurring, and the legitimacy of public policies should be found in the results and benefits they can produce for the community rather than in the strict respect of the legal framework.

In particular, it has become evident how the European integration is, in its deepest *raison d'être*, an instrument that must enable Europeans to achieve all the possible benefits of a more efficient allocation of goods and services.[56]

Any attempt to draw lines and boundaries between what is economic and what is not, what is competence of the Union, and what is responsibility of the Member States or subnational autonomies, thus poses the risk of losing the relevance of integration policies in responding to people's needs and overcoming social inequalities.[57]

Of course, the European Union has to act with legal titles, and it can't override the organizational structures set up by Member States. In this work, however, it has been possible to highlight how identifying innovative social goals such as e-Health can allow, even with limited legal titles, to start an institutional dialogue that makes multilevel governance a tool for integrating different competencies. In this sense, the presence of many institutional actors is not a cause of fragmentation. It can, actually, enable the construction of public interventions in order to adapt to the territorial differences existing in society.

However, the proper functioning of this model requires, at all levels of government, a broad willingness to conceive their role not as safeguarding widespread particularism but as a contribution to a genuine substantive equality.

[56] D. C. Mueller, *Constitutional Issues Regarding European Union expansion*, in B. Steunenberg (eds.), *Widening the European Union: Politics of Institutional Change and Reform*, London, New York, Routledge, 2003, 41.
[57] A. Biondi and O. Stefan, *EU Health Union*, 898.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp 17-31
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 03

*European Data Strategy. An Approach to the European Health Data Space. The Role of the Regulation (Eu) 2022/868 of the European Parliament and of the Council of May 30, 2022 Relating to European Data Governance**

Nieves de la Serna Bilbao
(Ph Dr. Administrative Law at Universidad Carlos III de Madrid)

Fernando Fonseca Ferrandis
(Ph Dr. Administrative Law at Universidad Carlos III de Madrid)

ABSTRACT European law has enshrined for years the dogma of the confidentiality of personal data. However, in recent years it wants to modulate the strict rules that configured this right and accepts certain data traffic. Along with reasons of general interest, it is not possible to forget the economic reasons.

1. *Problem planning*

As is well known, in recent years there has been a change of focus in the data protection policy developed in the European Union. From a practically absolute sacralization of the right to data protection, the aim is now to modulate the scope of this right in such a way that its material object, i.e. data, can be put to some use for the benefit of society - we are told-.[1] This, logically, articulating the actions taken by the Member States of the European Union from this perspective. In short, the aim is to create a single European data market and, at the same time, to develop common european data spaces, all in order to promote the exchange and sharing of data. It should be emphasized that these objectives are consistent with the Treaty on the Functioning of the European Union (TFEU), which provides for the creation of an internal market and the establishment of a system to prevent distortion of competition in this market. It should be emphasized that these objectives are consistent with the TFEU, which provides for the creation of an internal market and the establishment of a system to prevent distortion of competition in that market. Let us recall that the European Data Strategy (Communication of February 19, 2020) already envisaged a so-called common European data space in which data could be used regardless of where they were physically stored within the European Union. And within this common space, the creation of common European data spaces was proposed in specific areas and, specifically, in the field of health, a circumstance that more than justifies the treatment in this context of the DGA, since, let us remember that such data are nothing other than information content, in our case, health information.[2]

Specifically, the objective of the European Health Data Space (EHDS) is to establish a

* Article submitted to double-blind peer review.

[1] On this traditional perspective see L. Cristea Uivaru, *La protección de datos de carácter sensible: Historia clínica digital y big data en salud,* Bosch, Barcelona, 2019. Vv. Aa*., Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantías de los Derechos Digitales*, vol. I-II, Cizur Menor, Civitas/Thomson Reuters, 2021.

[2] J. Valero Torrijos, *La propuesta europea sobre gobernanza de los datos, ¿un paso adelante?* https://datos.gob.es/es/blog/la-propuesta-europea-sobre-gobernanza-de-los-datos-un-paso-adelante, 2020 and *Implicaciones jurídicas de los espacios de datos,* https://datos.gob.es/es/blog/implicaciones-juridicas-de-los-espacios-de-datos, 2023. Likewise, J. Valero Torrijos and R. Martinez Gutierrez (eds), *Datos abiertos y reutilización de la información del sector público*, Comares, Granada, 2022.

European governance framework - through the articulation of a series of common rules, criteria and practices - in relation to both a primary use of health data - use of health data to provide care to a subject - as well as with a secondary use of the same - use of data for research purposes or the development of public policies -. And from this perspective, the EHDS establishes a series of objectives aimed at this end; essentially the following: a) reinforce the patient's control over his or her data; b) regulate electronic health record systems so that they are trustworthy, secure and interoperable; c) regulate secondary use of data; d) establish two types of cross-border infrastructure depending on whether it is the primary use of secondary data or its secondary use. In short, as various authors have shown, this is a particularly ambitious policy because we are talking about specially protected data, subject to special regulation because it affects a more intimate area of the person. However, at the same time, adequate and coherent management of this information in electronic and interoperable format between the different health centers, whether they are from the same State of the European Union or from different ones, can be a benefit for the interested party themselves, for the industry and for the development of public policies.[3] We are therefore faced with the development of an essential policy given that - there is no doubt about this- the use of the economic and social potential of data - data economy - allows for a more correct and efficient reuse of the same, which, in turn, must facilitate the increase in the volume of data made available for the different uses that we mentioned above - and there is no doubt about this- taking advantage of the economic and social potential of data - data economy - allows for a more correct and efficient reuse of data, which, in turn, should facilitate the increase in the volume of data available for the different uses that we mentioned above. Note the potential that such a policy can have as a basis for transnational cooperation in certain fields of medicine such as transplantology;[4] it would be a decisive tool in the hands of organizations dedicated to the coordination of transplants such as the National Transplant Organization (ONT) or, at the European level, Eurotransplant.

However, the fact that it is ultimately about creating a market - of data and European but, in the end, a market -, a teleological purpose of whose reality is good proof of the normative provision of instrumental mechanisms - because they are at the service of the data policy analyzed in these brief pages and in which for-profit organizations can participate - and whose purpose even reaches to enable commercial use of the data obtained, raises important doubts of viability, legitimacy and legality.[5] Basically, due to the compatibility between what should be the development of a public policy such as the development and management of data protection, especially in an area such as health governed by the principle of objective service to the general interest and initiative. private sector whose cornerstone is, on the contrary and legitimately, its free development. A very basic example. When, in the context of regulated data exchanges, it is necessary to anonymize or a definitive dissociation of certain data, will the natural or legal person for commercial purposes act accordingly, in order to safeguard the right to data protection and take extreme precautions so that said anonymization or definitive dissociation is true and real? Regardless of even the economic cost of ensuring said result? Or, on the contrary, will you care more about your profits and therefore care less about the absolute protection of the right to data protection? Remember that we are talking about organizations that act for commercial purposes. We are certainly not talking about anything new. This is a problem that has manifested itself years ago in the different processes of privatization and deregulation of certain economic areas operated in all the countries around us and in which European law has had a resounding impact.[6] The new element is the area in which it is raised. As we already know, the field of data protection and,

[3] In this sense, see F. García Pérez*, Introducción al espacio europeo de datos sanitarios: un nuevo horizonte en la Gobernanza de Datos Sanitarios en la Unión Europea*, in *Actualidad Jurídica Uría Menéndez*, vol. 61, 2023, 183-196. Also, J. Marcus Scott, *The European Health Data Space, Think Tank European Parlament*, PE 740.054, December 2022.

[4] Concept used by R. Matesanz Acedos, *El milagro de los trasplantes*, Madrid, *La Esfera de los Libros S.L.*, 2006, 39.

[5] D. Ruano Delgado and N. Philipia, *Tratamiento seguro de datos como factor de integración europea: implicaciones legales en el ámbito de la salud pública en Georgia*, in *Revista de derecho y genoma humano*, no. 1, 2019, 525-546.

[6] On these issues see M.N. De La Serna Bilbao, *La privatización en España. Fundamentos Constitucionales y Comunitaruios*, Aranzadi, Pamplona, 1995.

in our case, in a particularly delicate area due to its relationship with our strictest personal privacy such as health.

On the other hand, even in the data exchange procedures that are developed based on the principle of altruism or gratuity - it would be good for the standard under development to specify the scope of said concepts - we are going to find that society - which is the source of all processed health data, whatever the scope of said treatment, will be deprived of the economic benefit produced by the mere possession of health data and which we can consider as "Informational Value." It is enough to know what happened in Iceland in the late 1990s to realize the magnitude of the problem. Indeed, it is not only that instruments are not provided to ensure that society also enjoys a certain return on achievements obtained with its data free of charge - this is not even considered. The enjoyment will be in the vast majority of cases through compensation, either direct, if the patient directly uses certain medical treatments - precisely those that derive from research developed from data obtained free of charge- or indirect, if the patient uses the benefits of public health services which, in turn, will have purchased the corresponding treatments from the different laboratories involved in the research. In accordance with the norm and apart from some health benefits that are a consequence of the development of certain public health policies, the only case in which citizens can avail themselves free of charge of the medical advances produced from the information that they themselves generate is that they participate in a clinical trial. There's no more. Surely, given the prevalence of community law, this paradigm shift must be accepted; that the right to our health data protection is not going to be what it was. But you have to be aware of it. However, it is surprising that this is the case, when the European Union has never played a relevant role in health matters.

In this context, Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and amending Regulation (EU) 2018/1714 (Data Governance Act) [DGA] makes sense, which seeks to introduce common standards and practices among the Member States of the European Union that allow the creation of a harmonized framework in which to develop a common data governance policy, in addition, fully respectful of fundamental rights.[7] In any case, it should be noted that the European data governance policy does not oblige public sector bodies to allow the transfer of data, nor does it exempt them from their confidentiality obligations. For this reason, the development of this policy should be without prejudice to the law of the European Union, the national law of each Member State or international agreements relating to the protection of the data that constitute the material object of the EDPR and to which the European Union or its Member States are party. Furthermore, the development of this policy should be without prejudice to European Union or national law on access to documents, as well as to the obligations of public sector bodies to authorize the re-use of data under European Union or national law of the Member States (art. 3.3 DGA).[8]

[7] About this question see A. Cerrillo i Martinez and M. Ascensión Moro Cordero, *El Reglamento de Gobernanza de Datos y su impacto en las administraciones públicas, Consultor de los ayuntamientos y de los juzgados*, in *Revista técnica especializada en administración local y justicia municipal*, no. 8, 2022, 1128-1135; C. Fernández Hernández*, Estructura y contenido del Reglamento (UE) 2022/868, de 30 de mayo, relativo a la gobernanza europea de datos o Reglamento de Gobernanza de Datos*, Diario La Ley nº 62 (Sección Ciberdecho), 7 de junio de 2022, Wolter Kluwer, 96; S. Leguinagoicoa García*, Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo Europeo y dle Consejo de 30 de mayo de 2022 relativo a la gobernanza europea de dato sy por el que se modifica el Reglametno (UE) 2018/1274 (Reglamento de Gobernanza de Datos)*, in *Revista Vasca de Gestión de Personas y Organizaciones públicas*, no. extra 5, 2023, 166-169; R. Martínez Martínez, *Data Governance Act: La construcción de un espacio europeo del dato*, in *Ley de Privacidad*, no. 9, 2021, 3 and R. Martínez Martínez, G. López Serrano, A. Padín Vidal and I. del Hoyo Alegria, *HealthData 29: un modelo de compartición de datos de investigación en salud en el contexto del futuro Espacio Europeo de Datos de Salud*, in *Comunicaciones en propiedad industrial y derecho de la competencia*, vol. 93, 2021, 5-30.

[8] It should be noted that the analyzed rule is without prejudice to Regulations (EC) n. or 223/2009, (EU) 2018/858 and (EU) 2018/1807, as well as Directives 2000/31/EC, 2001/29/EC, 2004/48/EC, 2007/2/EC, 2010/40/EU, (EU) 2015/849, (EU) 2016/943, (EU) 2017/1132, (EU) 2019/790 and (EU) 2019/1024 of the European Parliament and of the Council, and any other sectoral Union legislation regulating access to and re-use of data, as well as without prejudice to Union and national law on access to and use of data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, as well as international cooperation in that context. Likewise, the EDPR should be without prejudice to the competences of the Member States with

It should be noted that in this paper we focus our attention on the three central pillars of the regulation, i.e. the reuse of certain categories of data held by public sector bodies, the provision of data intermediation services and, finally, the transfer of data for altruistic purposes. In doing so, we wish to highlight these truly substantive institutions outside the regulation of other matters of a purely instrumental nature. Let us now analyze each of them.

2. *The Reuse of certain categories of data held by public sector organizations*

2.1. *Definition and material scope*

The European Union has traditionally considered that data generated from public budgets should benefit society. It is for that reason that Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and reuse of public sector information (DDA) mandates the public sector to make as much data as possible readily available for use and use. Despite that desire, there are certain categories of data - for the time being, commercially confidential data, data covered by statistical confidentiality, data protected by third party intellectual property rights and personal data - protected both by European Union law and by the domestic law of the Member States that are logically not available for general use.[9]

It is precisely these categories of data that constitute the object of the first of the three data transfer mechanisms analyzed. This concerns the reuse of certain categories of protected data held by public sector bodies, i.e. the use, by natural or legal persons, of such data for commercial or non-commercial purposes other than the initial purpose encompassed in the public service mission for which the data were produced. An exception is made for the exchange of data between public sector bodies for the sole purpose of carrying out their public service activities. Specifically, such a re-use mechanism applies to data protected for the following reasons:

a) Commercial confidentiality, including commercial, professional or business secrets.
b) Statistical confidentiality.
c) Protection of intellectual property rights of third parties.
d) Protection of personal data, insofar as such data are excluded from the scope of Directive (EU) 2019/1024.

In parallel, a significant number of categories of data are excluded from the material scope of the DGA; expressly the following categories of data:

a) Data held by public companies - given that these organizations are not part of the definition of public sector body.
b) Data held by public broadcasting organizations, and their subsidiaries, as well as data held by other organizations and their subsidiaries for the performance of a public service broadcasting mission.
c) Data kept by cultural centers - libraries,

regard to their activities in the field of public security, defense and national security. For example, the re-use of data protected on those grounds and held by public sector bodies, including data obtained in public procurement procedures falling within the scope of Directive 2009/81/EC of the European Parliament and of the Council, should not be covered by this Regulation.
Furthermore, the DGA is without prejudice to Regulations (EU) 2016/679 and (EU) 2018/1725 of the European Parliament and of the Council, as well as Directives 2002/58/EC and (EU) 2016/680 of the European Parliament and of the Council and corresponding provisions of national law, including personal data and non-personal data in a data set that are inextricably linked. In particular, the GDPR should not be interpreted as establishing a new legal basis for the processing of personal data for any of the regulated activities or modifying the information requirements provided for in Regulation (EU) 2016/679. Its application should not prevent cross-border transfers of data in accordance with the provisions of Chapter V of Regulation (EU) 2016/679. In the event of a conflict between the provisions of this Regulation and Union law on the protection of personal data or national law adopted in accordance with Union law on the matter, the Union or national law applicable in the matter should prevail.

[9] Thus, along with Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, we have to cite Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data and repealing Council Framework Decision 2008/977/JHA]. At the domestic level, it is necessary to abide by the provisions of Organic Law 3/2018, of December 5, on the Protection of Personal Data and Guarantee of Digital Rights and Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and enforcement of criminal penalties.

archives, museums, orchestras, operas, ballets and theaters - and educational institutions. In these cases, the works and other documents in their possession are mainly protected by the intellectual property rights of third parties.

d) Data kept for reasons of national security, defense or public safety.
e) Also excluded are data the provision of which is an activity outside the scope of the public service mission of the public sector bodies concerned as defined in the legislation or other binding rules of the Member State or, in the absence of such rules, as defined in accordance with the common administrative practice of that Member State, provided that the scope of the public service mission is transparent and subject to review.

It seems appropriate to specify, for the purpose of delimiting our object of study, that public sector organizations are understood to be any organization that meets the following characteristics:

a) First, it must have been created specifically to satisfy needs of general interest and not be of an industrial or mercantile nature;
b) Secondly, it must be endowed with legal personality;
c) Finally, it must be financed, for the most part, by State, regional or local authorities or other bodies governed by public law, the management of which is subject to the supervision of such authorities or bodies, or more than half of the members of its administrative, management or supervisory body must have been appointed by State, regional or local authorities or by other bodies governed by public law.

Although it does not seem necessary to have an impact on this issue, in our we have to be to the provisions of Law 40/2015, of October 1, on the Legal Regime of the Public Sector in order to finalize the concurrence in the specific case of such teleological, subjective and financial requirements.

It is, on the contrary, to specify that the data re-use regime must be applied to data whose provision is part of the entrusted public service mission - defined, case by case or in general - of the public sector bodies concerned, as provided for in the domestic legislation of the Member States. In the absence of such rules, the public service mission should be defined in accordance with the common administrative practice of the Member States, provided that the scope of the mission is transparent and subject to review. In any case, due to the nature of these data - sensitive data- the DGA subjects their transfer to strict compliance with legal and technical requirements, aimed at safeguarding the rights of the data subjects, which we analyze below.

2.2. *Applicable legal regime*

In determining how the re-use of data held by public sector bodies should be carried out, the essential idea of the European data governance policy is, as we already know, respect for competition law. For this reason, the conclusion of agreements that may have as their direct or indirect object the recognition of exclusive rights for the reuse of data must be avoided. This is provided for in Article 4.1 of the DGA when it expressly states "Agreements or other practices relating to the reuse of data held by public sector bodies containing categories of data in Article 3.1 granting exclusive rights or having the effect of granting exclusive rights or restricting the availability of the data for reuse by entities other than the parties to such agreements or practices are prohibited". Recall that the categories of data referred to in Article 3.1 of the DGA are those retained by public sector bodies that are protected for reasons related to commercial confidentiality, statistical confidentiality, intellectual property and personal data protection.

There is, however, a very qualified exception to this general rule. Indeed, where it is necessary for the provision of a service or a product of general interest, it is possible to grant an exclusive right for the re-use of this kind of data, where the provision of such a service or supply would otherwise not be possible (Art. 4.2 DGA). Recital 13 gives a concrete example of the legal provision and refers to the hypothesis that the exclusive use of the data is the only way to optimize its social benefits; for example, when there is only one entity - specializing in the processing of a specific set of data - capable of providing the service or offering the product that allows the public sector body to provide an advanced digital service in the interest of all. This possibility is equally plausible in the biomedical field where only a small number of laboratories or industries are able to articulate the highly complex treatments based on artificial intelligence. In any case, the recognition of such exclusive rights is not

free. It can be done by means of an administrative act or contractual provision but in accordance with the applicable Union or national law of the Member States - including the relevant State aid rules - and in compliance with the principles of transparency, equal treatment and non-discrimination (Art. 4.3 DGA).

These are not the only precautions established in this regard. The following should also be noted:

a) First, the maximum duration of an exclusive right to reuse data is twelve months, which is a substantial reduction with respect to the period initially in the proposal, which was three years. This is a provision that is more in line with the general rule and with the principle of competition. When a contract is concluded, the duration of the contract must be the same as that of the exclusive right (art. 4.4 DGA).
b) The granting of an exclusive right in application of the above considerations - including the reasons why it is necessary to grant it - must be made in a transparent manner and must be publicly disclosed online, in a manner consistent with the relevant Union law on public procurement (Art. 4.5 DGA).
c) Agreements should be subject to a periodic review based on a market analysis in order to determine whether such exclusivity is still necessary.

Where an exclusive right to re-use data does not comply with this Regulation, such exclusive right should be considered as null and void.

On the other hand, it should be emphasized that since the re-use of some categories of protected data - we already know, those referred to in Art 3.1) DGA- constitutes the teleological element of the European Data Governance Policy and given, also, that the development of the same cannot be developed freely except in accordance with the provisions of the European Union and of the Member States themselves, it seems clear that a core element of such a policy must be the establishment of the criteria or conditions to be met in order to make possible the intended reuse of data, aimed at protecting the rights and interests of third parties, safeguarding the interests of those who reuse the data and without this entailing a disproportionate effort for the public sector. Such regime is understood, moreover, without prejudice to the rights and obligations of the regime of access to such data

Public sector bodies which, under national law, are competent to grant or refuse access for re-use of one or more of the categories of data referred to in Article 3.1) of the DGA must publish the conditions under which re-use is allowed. For this purpose, they may be assisted by the competent bodies referred to in Article 7.1). In addition, Member States must ensure that the public sector bodies referred to have the means and resources to perform this function. It is, therefore, an instrumental obligation - insofar as it is aimed at making the conditions for the re-use of data feasible - but, at the same time, directly related to legal certainty.

As regards the actual wording of the conditions for reuse, it should be pointed out that, in general, they must be non-discriminatory, proportionate, objectively justified in terms of the categories of data, the purposes of reuse and the nature of the data in question and, furthermore, they may not be established to restrict free competition. However, public sector bodies may impose the use of certain technical means aimed - exclusively - at guaranteeing the rights and interests of third parties in relation to the data. Hence, the possibility of imposing the obligation that only pre-processed data be used for re-use, when the purpose of the pre-processing is to anonymize or pseudonymize personal data or to delete confidential commercial information, in particular trade secrets.

Likewise, public sector bodies must ensure, in accordance with Union and national law, that the protected nature of the data is preserved and, in this regard, may impose the following obligations:

a) That access for re-use of the data is granted only where the public sector body or competent body, following a request for re-use, has ensured that the data have been anonymized, in the case of personal data, and modified, aggregated or processed by any other method of disclosure control, in the case of commercially sensitive information, including trade secrets or proprietary content.
b) That the remote access and reuse of the data is carried out in a secure processing environment provided or controlled by the public sector body.

c) That the access and re-use of the data is carried out in the physical premises where the secure processing environment is located in accordance with strict security standards, provided that remote access cannot be enabled without jeopardizing the rights and interests of third parties.

Where re-use is permitted - in accordance with paragraph 3 b) and c) above- public sector bodies should impose conditions that preserve the integrity of the functioning of the technical systems of the secure processing environment used. The public sector body must reserve the right to verify the process, means and results of data processing carried out by the reuser in order to preserve the integrity of data protection and must reserve the right to prohibit the use of those results that contain information endangering the rights and interests of third parties. The decision to prohibit the use of the data must be understandable and transparent to the reuser.

3. *Data Exchange Services*

3.1. *Definition and material scope*

The DGA establishes a comprehensive legal regime applicable to data intermediation activities, which is generally applicable except in the case of recognized data management organizations for altruistic purposes or other non-profit entities, provided that their activities consist of the collection of data provided for altruistic purposes by natural or legal persons for the fulfillment of general interest purposes. This exception to the general rule does not apply, however, when the purpose of such organizations and entities is to establish commercial relations between an undetermined number of data subjects and data owners, on the one hand, and data users, on the other. Well then, going into the matter properly, it should be stated that, in accordance with the provisions of the DGA, the following services are considered to be data intermediation services:

a) Intermediation services between data owners and potential data users, including the provision of technical or other means to enable such services. These services may include the bilateral or multilateral exchange of data or the creation of platforms or databases that enable the exchange or sharing of data, as well as the establishment of other specific infrastructure for the interconnection of data owners with data users;
b) Intermediation services between data subjects wishing to provide their personal data or natural persons wishing to provide non-personal data and potential data users, including the provision of the technical or other means necessary to enable such services, and in particular to enable the exercise of data subjects' rights provided for in Regulation (EU) 2016/679;
c) Finally, Data cooperative services. We still don't know very well how this system will operate.

3.2. *Applicable legal regime*

It should then be noted that the above-mentioned intermediation services are also subject to a notification procedure, the regime of which is described below. It should be noted that any data brokering service provider intending to provide the data brokering services referred to above (Article 10 DGA) must submit a notification to the competent authority for data brokering services. According to the text of the DGA, this is an unavoidable obligation; only after the data brokering service provider has submitted the notification can it start its activity, and it should be noted that it entitles it to provide data brokering services in all EU Member States. For these purposes, a data brokering service provider established in more than one Member State is considered to be subject to the legal system of the Member State of its main establishment, without prejudice to Union law governing cross-border actions for damages and related proceedings. Providers of data brokering services which are not established in the Union and which offer in the Union the data brokering services referred to in Article 10 of the DGA must appoint a legal representative in one of the Member States in which such services are offered.[10]

[10] In accordance with the provisions of Article 11 DGA "For the purposes of this Regulation, a data intermediation services provider with establishments in more than one Member State shall be deemed to be under the jurisdiction of the Member State in which it has its main establishment, without prejudice to Union law regulating cross-border actions for damages and related proceedings". Likewise "The data intermediation services provider shall be deemed to be under the jurisdiction of the Member State in which the legal representative is located. The designation of a legal representative by the data intermediation services provider shall be without prejudice to any legal actions which could be initiated against the data intermediation services provider".

The notification must include the following information:

a) Name of the data brokering service provider.
b) The legal nature of the data brokering service provider, as well as its legal form, ownership structure, relevant subsidiaries and, where the data brokering service provider is registered in a commercial register or similar national public register, its registration number.
c) Address of any principal place of business of the data brokering service provider in the Union and, where applicable, of any branch in another Member State, or address of its legal representative.
d) Public website containing complete and up-to-date information on the data brokering service provider and on its activities, including at least the information referred to in points a), b), c) and f) of Article 11 of the DGA.
e) Contact persons of the data brokering service provider and contact details.
f) Description of the data brokering service that the data brokering service provider intends to provide and indication of the categories listed in Article 10 to which the data brokering service corresponds.
g) An estimate of the date of commencement of the activity, if different from the date of notification.

Likewise, any modification of the information submitted must be notified, as well as the cessation of activity.

The competent authority for data intermediation services is subject to a series of obligations to be fulfilled at the request of the data intermediation service provider. First, it must issue - within one week of the notification being duly and fully submitted - a standardized statement confirming that the data brokerage service provider has submitted the notification and that the notification contains the required information. Secondly, it must confirm that the data brokerage service provider complies with the provisions of the DGA. Only thereafter, upon receipt of such confirmation, the data brokerage service provider may now use, in its oral and written communications, the designation "data brokerage service provider recognized in the Union", as well as a common logo. Finally, it must inform the Commission electronically and without delay of each new notification. To this end, the Commission must keep a regularly updated public register of all data brokering service providers providing services in the Union. The information required in paragraph 6 a), b), c), d), f) and g) must be published in the public register. In any case, the competent authority for data brokering services must ensure that the notification procedure is non-discriminatory and must not distort competition.

Apart from the above, the provision of data brokering services by the relevant providers is subject to compliance with the following conditions:

a) They may not use the data in relation to which they provide their services for purposes other than making them available to data users and shall provide the data brokering services through a separate legal entity.
b) The commercial contractual terms, including those relating to pricing, for the provision of data brokering services to a data subject or data user may not depend on whether the data subject or data user uses other services provided by the same data brokering service provider or by an entity related to it, and, if used, may not depend on the extent to which the data subject or data user uses such services.
c) Data collected on any activity of a natural or legal person for the purpose of providing a data brokering service, including date, time and geolocation, duration of the activity and connections that the user of the data brokering service establishes with other natural or legal persons, may only be used for the performance of that data brokering service, which may involve the use of data for fraud detection or cybersecurity purposes and must be made available to data subjects upon request.
d) Data should be exchanged in the same format in which they are received from the data subject or data owner. As an exception to this general rule, specific formats may only be adopted for the purpose of improving intra- and inter-sectoral interoperability; when requested by the data user; if required by Union law; or when necessary for the purpose of harmonization with international or European data standards. In all such cases, data subjects or data subjects should be offered an opt-out possibility in relation to

such conversions, unless such conversion is required by Union law; or where necessary for the purpose of harmonization with international or European data standards. In all such cases, data subjects or data subjects should be offered an opt-out possibility in relation to such conversions, unless such conversion is required by Union law.

e) Data brokering services may include the offer of additional specific tools and services to data subjects or data subjects for the specific purpose of facilitating the exchange of data, for example, temporary storage, organization, conversion, anonymization and pseudonymization, provided that such tools and services are only used upon the express request or approval of the data subject or data subject and that the third-party tools offered in this context are not used for other purposes.
f) It should be ensured that the procedure for access to data brokering services, including prices and terms of service, is fair, transparent and non-discriminatory, both for data subjects and for data subjects and data users.
g) Data brokering services should have procedures in place to prevent fraudulent or abusive practices by parties seeking access through their data brokering services.
h) Providers of data brokering services should ensure, in the event of insolvency, reasonable continuity in the provision of their data brokering services and, where such data brokering services include the storage of data, should have in place the necessary safeguards to enable data subjects and data users to access, transfer or retrieve their data and, where they provide such data brokering services between data subjects and data users, to enable data subjects to exercise their rights;
i) appropriate measures should also be taken to ensure interoperability with other data brokering services, inter alia, through open standards commonly used in the industry in which data brokering service providers operate.
j) Data brokering service providers should implement appropriate technical, legal and organizational measures to prevent access to or transfer of non-personal data where such access or transfer is unlawful under Union law or the national law of the Member State concerned.
k) Data subjects should be informed without delay in case of unauthorized transfer, access or use of non-personal data that they have shared.
l) Necessary measures must be taken to ensure an adequate level of security in relation to the storage, processing and transmission of non-personal data. Likewise, they must ensure the highest level of security in relation to the storage and transmission of competitively sensitive information.
m) Where data brokering service providers offer services to data subjects, they should act in the best interests of the data subjects when facilitating the exercise of their rights, in particular by informing and, where appropriate, advising them in a concise, transparent, intelligible and easily accessible manner about the intended uses of the data by data users and the general conditions applicable to such uses before the data subjects give their consent.
n) Where data brokering service providers provide tools to obtain data subjects' consent or permission to process data provided by data subjects, they shall specify - where applicable - the territory of the third country in which the data are intended to be used and shall provide data subjects with tools both to grant and withdraw their consent, and data subjects with tools both to grant and withdraw permissions to process data.
o) Finally, data brokering service providers must keep a record of the data brokering activity artificial intelligence

In any case, the competent authorities for data intermediation services must control and supervise compliance with the requirements to be met by data intermediation service providers. Likewise, at the request of a natural or legal person, they may control and supervise such compliance by data brokering service providers. To this end, they are empowered to request from data brokering service providers or their legal representatives any information necessary in order to verify compliance with the requirements of this Chapter. Requests for information must be proportionate to the performance of their duties and be reasoned. To this end, the DGA provides that when the competent authority for data intermediation services considers that a data intermediation service provider does not comply with one or more of the requirements of this chapter, it must notify it

of its observations and the latter must express its opinion on the matter within thirty days of receipt of the notification. Likewise, the competent authority for data intermediation services is empowered to require the cessation of infringements involving non-compliance with the legal requirements within a reasonable period of time or, in the case of serious infringements, immediately, taking appropriate and proportionate measures to ensure compliance. In this regard, the competent authority for data intermediation services is empowered to adopt the following measures:

a) Impose, through administrative proceedings, dissuasive financial penalties, which may include periodic penalty payments and penalties with retroactive effect, initiate legal proceedings for the imposition of fines, or both.
b) Require a postponement of the commencement or a suspension of the provision of the data brokering service until the conditions have been modified as requested by the competent authority for data brokering services.
c) Demand the cessation of the provision of the data brokering service in case of serious or repeated breaches that have not been corrected despite prior notification.

In such cases, the competent authority for data brokering services must request the Commission to cancel the registration of the data brokering service provider from the register of data brokering service providers, once it has ordered the cessation of the provision of the data brokering service. However, if the data brokering services provider remedies the infringements, it may make a new notification to the competent data brokering services authority, which must be communicated by the competent data brokering services authority to the Commission.

In adition, it should also be noted that where a data brokering services provider that is not established in the Union fails to designate a legal representative or the legal representative of the latter fails to provide, upon request of the competent data brokering services authority, the necessary information comprehensively demonstrating compliance with the DGA, the competent data brokering services authority may postpone the commencement or suspend the provision of the data brokering service until a legal representative is designated or the necessary information is provided. These authorities must promptly notify the data brokering service provider concerned of the measures imposed, the grounds on which they are based and the necessary measures to be taken to remedy the deficiencies concerned, and set a reasonable period of time, not exceeding 30 days, for the data brokering service provider to comply with the measures imposed.

If the principal establishment or the legal representative of a data brokering services provider is located in a given Member State but the provider provides its services in other Member States, the competent authority for data brokering services of the Member State of its principal establishment or in which its legal representative is located and the competent authorities for data brokering services of the other Member States shall cooperate with each other and provide mutual assistance. Such assistance and cooperation may cover the exchange of information between the competent authorities for data brokering services concerned for purposes related to their functions under the GDPR and reasoned requests for the measures referred to in the DGA to be taken.

It should be noted that where a competent authority for data intermediation services of one Member State requests assistance from a competent authority for data intermediation services of another Member State, it must submit a reasoned request. The competent data intermediation authority receiving such a request shall respond without delay and within a time limit proportionate to the urgency of the request.

4. *The Altruistic Transfer of Data*

4.1. *Definition and material scope*

Irrespective of all the above possibilities, the DGA nevertheless facilitates the transfer of certain types of data when such transfer is altruistic in nature and therefore free of charge. To this end, the DGA establishes a general empowerment in the sense that the Member States may establish organizational and/or technical provisions to facilitate the altruistic transfer of data, and may even draw up national policies on the altruistic transfer of data aimed at assisting data subjects in the voluntary transfer, for altruistic purposes, of personal data relating to them held by public sector bodies and at establishing the necessary

information to be provided to data subjects in relation to the re-use of their data for purposes of general interest. To this end, the DGA establishes a series of provisions that we analyze below.

4.2. *Applicable legal regime*

All authorities competent for the registration of data management organizations for altruistic purposes must periodically update a national public register of recognized data management organizations for altruistic purposes. Provided that the entities are entered in the national public register of recognized data management organizations for altruistic purposes, they may use, in their oral and written communications, the designation "data management organization for altruistic purposes recognized in the Union", as well as a common logo.[11] Likewise, the Commission should keep a public register of recognized data management organizations for altruistic purposes in the Union, albeit for information purposes.

In any case, in order for data management organizations for altruistic purposes to be entered in a national public register, they must meet the following requirements:

a) Exercise altruistic data transfer activities.
b) be a legal entity established under national law to fulfill objectives of general interest, as provided for in national law, where applicable.
c) It shall operate on a not-for-profit basis and shall be legally independent of any entity operating on a for-profit basis.
d) To carry out the altruistic data transfer activities through a structure that is functionally separate from its other activities.
e) Comply with the regulatory code referred to in Article 22, paragraph 1, no later than eighteen months after the date of entry into force of the delegated acts referred to in that paragraph.

It should also be noted that any entity that meets the requirements of Article 18 of the analyzed rule may apply for registration in the national public register of recognized data management organizations for altruistic purposes in the Member State in which it is established. In addition, when these entities have establishments in more than one Member State, they may apply for entry in the national public register of recognized data management organizations for altruistic purposes in the Member State in which they have their main establishment. In the case of entities that meet the requirements of Article 18 but are not established in the Union, they must designate a legal representative in one of the Member States in which they offer their altruistic data management services.

For the purpose of ensuring compliance with the DGA, the entity must give a mandate to the legal representative to be addressed by the competent authorities for the registration of data management organizations for altruistic purposes or by data subjects and data subjects instead of or in addition to the entity, in all matters concerning the entity. From this perspective, the legal representative has to cooperate with the competent authorities for the registration of data management organizations for altruistic purposes and must demonstrate to them in a comprehensive manner, upon request, the measures and arrangements taken by the entity to ensure compliance with the DGA. The entity is deemed to be subject to the legal system of the Member State in which its legal representative is located. Such an entity may apply for registration in the national public register of recognized data management organizations for altruistic purposes in that Member State. The designation of a legal representative by the entity should be without prejudice to any legal action that may be brought against the entity.

The applications for registration referred to in the preceding paragraphs should include the following data:

a) Name of the entity.
b) Legal nature of the entity, as well as its legal form and, when it is registered in a national public registry, its registration

[11] Let us remember that in accordance with the provisions of Article 17 DGA "The Commission shall maintain a public Union register of recognised data altruism organisations for information purposes. Provided that an entity is registered in the public national register of recognised data altruism organisations in accordance with Article 18, it may use the label 'data altruism organisation recognised in the Union' in its written and spoken communication, as well as a common logo […]. In order to ensure that recognised data altruism organisations are easily identifiable throughout the Union, the Commission shall, by means of implementing acts, establish a design for the common logo. Recognised data altruism organisations shall display the common logo clearly on every online and offline publication that relates to their data altruism activities. The common logo shall be accompanied by a QR code with a link to the public Union register of recognised data altruism organisations".

number.
c) Statutes of the entity, if applicable.
d) Sources of income of the entity.
e) Address of any principal establishment of the entity in the Union and, where appropriate, of any branch in another Member State, or address of its legal representative.
f) Public website containing complete and up-to-date information about the entity and its activities, including at least the information referred to in points a), b), d), e) and h) above.
g) The entity's contact persons and contact details.
h) Objectives of general interest that the entity intends to promote with the collection of the data.
i) Nature of the data that the entity intends to control or process and, in the case of personal data, indication of the categories of personal data.
j) Any other document evidencing compliance with the requirements of Article 18.

Once the entity has submitted all this information and once the competent authority for registration of data management organizations for altruistic purposes has assessed the application for registration and found that the entity meets the requirements, the authority must proceed to register the entity in the national public register of recognized data management organizations for altruistic purposes within twelve weeks after receipt of the application for registration and must be notified to the Commission. In addition, it must be included in the Union's public register of recognized data management organizations for altruistic purposes. The registration is valid in all Member States.

In any case, the recognized data management organizations for altruistic purposes must notify the corresponding competent authority for entry in the register of data management organizations for altruistic purposes of any modification of the information submitted within fourteen days from the day of the modification. Likewise, the competent authority for the registration of data management organizations for altruistic purposes has to inform electronically and without delay the Commission of each such notification which must update without delay the Union public register of recognized data management organizations for altruistic purposes.

For the purposes of compliance with the transparency policy, it should be noted that the DGA establishes a twofold obligation for recognized data management organizations for altruistic purposes. On the one hand, they must keep a complete and accurate record of the following elements:
a) All natural or legal persons who have been permitted to process data held by that recognized data management organization for altruistic purposes, and their contact details.
b) The date or duration of the processing of personal data or the use of non-personal data.
c) The purpose of the data processing declared by the natural or legal persons to whom the data processing has been permitted.
d) Any fees paid by the natural or legal persons carrying out the data processing.

Irrespective of the above, the aforementioned organizations must prepare and transmit to the relevant authority competent for registration in the register of data management organizations for altruistic purposes an annual activity report, which must include at least the following data:
a) Information on the activities of the recognized data management organization for altruistic purposes.
b) A description of the manner in which the general interest purposes for which the data were collected have been promoted during the financial year in question.
c) List of all natural and legal persons who have been allowed to process data held by the entity, including a brief description of the general interest purposes pursued by the processing of the data and a description of the technical means employed for this purpose, with a description of the techniques applied to preserve privacy and data protection.
d) Summary of the results of the data processing permitted by the recognized data management organization for altruistic purposes, if applicable.
e) Information on the sources of income of the recognized non-profit data management organization, in particular, all income derived from providing access to the data, and on its expenses.

Specific requirements to protect the rights and interests of data subjects and data owners

with regard to their data.

All recognized data management organizations for altruistic purposes must also inform data subjects or data subjects, in a clear and easy to understand manner, prior to any processing of their data, about two circumstances. First, about the general interest purposes and, where appropriate, the specific, explicit and legitimate purposes for which the personal data will be processed, and for which they allow their data to be processed by a data user. Secondly, in relation to the location of any processing activity carried out in a third country and the general good purposes for which it is permitted, where the processing is carried out by the recognized altruistic data management organization itself. Data obtained by such organizations should not be used for purposes other than those in the general interest for which the data subject or data subject permits the processing, nor should they use misleading marketing practices to solicit the provision of data. They must provide tools to obtain data subjects' consent or permission to process data provided by data subjects and also provide tools to easily withdraw such consent or permission.

Whatever the case, these organizations must take the necessary measures to ensure an adequate level of security in relation to the storage and processing of non-personal data that they have collected for the purpose of altruistic data transfer. And, from the same perspective, they must inform data subjects without delay in case of unauthorized transfer, access or use of the non-personal data they have shared. It should be emphasized that when the recognized altruistic data management organization facilitates the processing of data by third parties, in particular by providing tools to obtain the consent of data subjects or permission to process data provided by data subjects, it shall specify, where appropriate, the territory of the third country in which the data are intended to be used.

It is foreseen that by means of delegated acts issued by the Commission, a regulatory code complementary to the DGA will be created, which for these purposes should be comprehensive of the following issues:

a) Adequate information requirements to ensure that data subjects and data subjects are provided, prior to granting their consent or permission for altruistic data transfers, with sufficiently detailed, clear and transparent information on the use of the data, the tools for granting and revoking consent or permission, and the measures taken to prevent misuse of data shared with the data management organization for altruistic purposes.
b) Adequate technical and security requirements to ensure an appropriate level of security of data storage and processing, as well as tools for granting and withdrawing consent or permission.
c) Communication roadmaps adopting a multidisciplinary approach to raise awareness among relevant stakeholders, in particular data subjects and data subjects who might share their data, about altruistic data sharing, the designation as a "Union-recognized altruistic data management organization" and the regulatory code.
d) Recommendations on relevant interoperability standards. Competent authorities for the registration of altruistic data management organizations.

The competent authorities for the registration of data management organizations for altruistic purposes are those designated by each Member State and must comply with the general requirements established by the DGA. The identity of each of these authorities, as well as their subsequent modification, must be notified to the Commission. In any case, they must perform their functions in cooperation with the relevant data protection authority, where such functions relate to the processing of personal data, and with the relevant sectoral authorities of that Member State.

It should be noted that these authorities are also the competent bodies to monitor and supervise compliance with the requirements of the DGA by recognized data management organizations for altruistic purposes, either ex officio or at the request of a party. To this end, they are also empowered to request from the recognized data management organizations for altruistic purposes all the information necessary to verify compliance with the requirements of regulation analyzed in these brief pages. In this regard, it provides that when a competent authority for the registration of data management organizations for altruistic purposes considers that a recognized data management organization for altruistic purposes does not comply with one or more of the requirements provided for in the DGA, it must notify it of its observations and grant it a period - of thirty days from the

receipt of the notification - to express its opinion on the matter. If a breach is found to exist, it may require cessation of the breach, either immediately or within a reasonable period of time, and must take appropriate and proportionate measures to ensure compliance.

Recognized altruistic data management organizations that fail to comply with one or more of the requirements determined in the DGA, even after having received from the competent authority for registration in the register of altruistic data management organizations is subject to the following consequences:

a) Loss of the right to use the denomination "data management organization for altruistic purposes recognized in the Union", in its oral and written communications;
b) Cancellation of its registration in the corresponding national public register of recognized data management organizations for altruistic purposes and in the Union public register of recognized data management organizations for altruistic purposes.

In any case, it should be noted in this regard that decisions to revoke the right to use the name of a data management organization for altruistic purposes must be made public. In addition, it should be specified that where a recognised altruistic data management organisation has its head office or its legal representative in a Member State but carries on its activities in other Member States, the competent authority for entry in the register of altruistic data management organisations of the Member State of its head office or legal representative and the competent authorities for entry in the register of altruistic data management organisations of those other Member States should cooperate with each other and assist each other. Such assistance and cooperation may cover the exchange of information between the competent authorities for the registration of the data management organisations for altruistic purposes concerned for purposes related to their tasks under European regulation and to reasoned requests for appropriate measures to be taken. All information exchanged in the context of the request and the provision of assistance should be used only in relation to the matter for which it was requested.

Finally, it should be noted that in order to facilitate the collection of data transferred for altruistic purposes, a "European Consent Form for Altruistic Data Transfer" - adopted by Commission delegated acts - is foreseen to enable data subjects to prove consent and its withdrawal in respect of a specific data processing operation in accordance with the requirements of Regulation (EU) 2016/679. The form should be made available in a way that allows it to be printed on paper and is easy to understand, as well as in an electronic and machine-readable format. Furthermore, it must allow its adaptation to specific sectors and different purposes.

5. *Conclusion*

European Data Governance and specifically in the field of health data, has proceeded to rethink its core ideas that have traditionally informed it. In effect, the new community rules aim to create a European data market - based on the so-called common European spaces - that allow the exchange of data and its sharing - we are told - in a manner that is fully respectful of the fundamental rights of the person. With this objective, the DGA has foreseen three legal mechanisms of different scope and intention but that can operate complementary, such as the Reuse of certain categories of data held by public sector organizations, the Data Exchange Services and the Altruistic Transfer of Data.

It is necessary to highlight that these data exchange systems introduce different elements of the market and that they give rise to private initiative, which, while not objectionable in themselves, while they can effectively contribute to energizing the data market, can introduce important distortions. in the operation of what a data protection policy should be, especially in an area as delicate as health. Indeed, as such a market will be governed by the expectation of profit. There is no need to be deceived in this assessment. However, remember that, in our case, we are talking about a special category of data due to its greater connection with the personal privacy of the person and, for this reason, it has traditionally enjoyed reinforced protection.

Experience shows that it is very difficult to marry public policy - data protection and health - and private interest. The stimuli of both, general interest, on the one hand, and free development and benefit, on the other hand, are in themselves contradictory. In our case, it is clear that the general interest must

prevail. But this is how it is combined with the spirit of the norm. On the other hand, when medical data is made available to some of the private organizations provided for by data intermediation systems, for example, in the reuse of certain categories of data held by public sector organizations - when organizations act for commercial purposes -, an additional economic value that society has generated and from which it will not be able to benefit is directly attributed to the private sector. There are only well-intentioned and highly ethereal claims that the progress generated by this data exchange will benefit society. No concreteness.

In short, from our perspective, only data exchange systems are viable in the field of health where the altruistic spirit prevails and where society is rewarded for the use of data that it itself has generated.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 33-48
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 04

*Regulation of Artificial Intelligence in Healthcare within the European Union**

José Vida Fernández
(Professor of Administrative Law at University Carlos III de Madrid)

ABSTRACT The use of artificial intelligence (AI) is spreading rapidly in healthcare. AI systems have no regulation of their own in the European Union, but are subject to a growing set of overlapping regulations that are difficult to identify and systematize. This paper provides an orderly analysis of all these regulations at the European level in order to clarify the cardinal points of the regulation of AI systems in healthcare, as it is not homogeneous, but depends on the specific use of the system. The new EU's Regulation on AI and the Regulation on Medical Devices are the two key points that should complement each other. However, they are insufficient as the AI Regulation is too generic and the Medical Devices Regulation is outdated. Therefore, a specific regulation is needed to regulate the use of AI in healthcare.

1. *Artificial intelligence in the European Union's new digital policy*

Nearly a decade ago, the European Union shifted its strategy in digital policy.[1] Previously, the Union favored a non-regulatory approach to digital innovation, allowing technological progress to develop freely. Regulation was basically based on corrective, negative, reactive and *ex post* measures. This approach facilitated significant advances such as the personal computer and the Internet, which developed under minimal intervention on specific issues such as privacy, intellectual property and consumer rights.[2]

At the beginning of the last decade, a shift in the model was initiated due to the increasing significance of the digital transformation for both economic growth and social development, as well as the imperative to foster an environment of trust and security. This change stemmed from the emergence of a new generation of data-protection regulation.[3] This regulation introduced proactive, *ex ante* measures aimed at prevention, actively engaging individuals in compliance (proactive responsibility). It adjusted the level of intervention based on the scale and severity of the risks (risk-oriented approach) and incorporated obligations from the outset (protection by design and by default). Additionally, it introduced supplementary measures such as self-regulation (codes of conduct) and co-regulation (certifications).

These new measures were applied across the entire digital sector, marking a departure from the traditional laissez-faire approach to digital policy. This shift is evident in the regulation of large platforms, such as the Digital Services Act and the Digital Markets Act, which introduce *ex ante* regulations.[4] However, the most notable change can be observed in the regulation of artificial intelligence (AI). For the first time, restrictions and limitations are imposed on the use of a digital innovation. AI regulation includes the most innovative and intensive instruments within the new EU digital policy as a response to its penetration

* Article submitted to double-blind peer review.
This paper is part of the research project "Artificial Intelligence in the national health care system: solutions to specific legal problems" (PID2021-128621NB-100), directed by José Vida Fernández and founded by the Ministry of Science and Innovation of Spain (MCIN/AEI/10.13039/501100011033/) and by "FEDER: A way of making Europe".

[1] On the origin of this change see U. Beck, *The Digital Freedom Risk: Too Fragile an Acknowledgment*, in *Quaderns de la Mediterrània*, no. 22, 2015, 141-144. Also see J. Vida, *The Risk of Digitalization: Transforming Government into a Digital Leviathan*, in *Indiana Journal of Global Legal Studies*, vol. 30, no. 2, 2023, 3-13. On the peculiarity of the European strategy for regulating digital innovation and its impact on innovation see A. Bradford, *The False Choice Between Digital Regulation and Innovation*, European University Institute, 2024.

[2] This explains why there has not been a piece of legislation like a Personal Computer Act or an Internet Act. The closest thing to the latter has been Directive 2000/31/EC on certain legal aspects of information-society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), which states that Member States may not restrict the freedom to provide information-society services of another Member State (art. 3).

[3] Specifically, Regulation (EU) 2016/679 of 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[4] These are Regulation (EU) 2022/2065 on a single market for digital services (Digital Services Act) and Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector (Digital Markets Regulation), and other regulations that make up the new digital-services package.

and disruptive potential.

According to the legal definition contained in the Regulation on Artificial Intelligence (RIA), [5] AI systems are software based on new forms of programming[6] that endow them with hitherto unknown functionalities, such as the capacity to generate predictions, contents, recommendations or decisions.

These systems are no longer linear, proposing solutions in a deterministic way, but have a certain autonomy although they are not independent, since they solve specific problems according to previously defined objectives.[7] AI systems are structured in various modalities, spanning from foundational models (generative AI) capable of executing multiple tasks (such as summarizing, responding, supervising, etc.) to highly specialized programs tailored for specific functions (like e-mail spam filters). Additionally, AI systems can be manifested in different forms. They can either function directly as software or be incorporated into robotic devices (such as articulated arms or vehicles), enabling them to translate their actions into physical responses by interacting with the environment.

The distinct attributes of AI, coupled with its rapid advancement and increasing ubiquity, have led to the implementation of various regulatory strategies at both the international and national levels.[8] The EU has been at the forefront of this movement, issuing a series of documents that have culminated in the Regulation on Artificial Intelligence (RIA) and the proposal for a Directive on AI liability[9] within a particularly short timeframe. These initiatives will be complemented by additional regulations addressing matters such as intellectual property rights, military applications, and more.

The European strategy on AI is unique as it does not solely rely on regulations but incorporates several soft-law instruments that provide a more flexible, agile and precise approach. They contain policy declarations on digital rights, which although not directly enforceable, offer guidance and serve as interpretative frameworks. Additionally, ethical guidelines, which preceded the Regulation now complement it. Furthermore, standardization plays a crucial role as a private and voluntary tool essential for managing this specialized and changing sector.

AI governance encompasses a comprehensive package of measures, comprising both traditional regulations and soft-law approaches. This comprehensive approach stands in contrast to the limited initiatives taken in the governance of other disruptive technologies such as blockchain, cloud computing, virtual reality, quantum computing, etc.

2. *The impact of artificial intelligence on healthcare*

The healthcare sector is experiencing a surge in the adoption of AI. This is due in part to the vast amount of data generated within the healthcare systems, which allows AI to be trained on a wealth of scientific evidence.[10]

[5] Regulation (EU) 2024 laying down harmonized rules on artificial intelligence defines AI systems as "a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (art. 3 RIA). Although the Commission's proposal referred to "software" and the final version opts for "machine-based systems" – probably to make it more generic –, AI system will generally consist of software. For an approach to AI legal definition see J. Vida Fernández, *Artificial Intelligence in Government: Risks and Challenges of Algorithmic Governance in the Administrative State*, in *Indiana Journal of Global Legal Studies*, vol. 30, no. 2, 2023, 73-75.

[6] Specifically, these are techniques based on machine-learning strategies, logic-based strategies, statistical strategies, etc. Unlike classical programming, in which systems receive data and rules to obtain results, AI systems receive data and results to define the rules that solve the problems posed, which gives them new functionalities.

[7] This specific AI (or narrow AI) is different from general AI (or strong AI) that characterizes human beings, which is not yet far from being achieved. See A. Zlotnik, *Artificial Intelligence in Public Administrations: Definitions, Project Feasibility assessment and Application Areas*, in *Boletic*, no. 84, 2019, 27–28. See also S. C. Kantheti and R. Manne, *Application of Artificial Intelligence in Healthcare: Chances and Challenges*, in *Current Journal of Applied Science and Technology*, no. 40, 2021,78-89.

[8] In the United States, President Biden issued Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence on October 30, 2023. Section 8 is specifically dedicated to the protection of patients (Sec. 8. Protecting Consumers, Patients, Passengers, and Students).

[9] The Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) COM/2021/206 final was submitted on April 21, 2021 and has been adopted in three years. As for the Proposal for a Directive from the non-contractual liability rules to artificial intelligence (AI Liability Directive) COM/2022/496 final was submitted on September 28, 2022 and continues to be processed.

[10] In this sense, William Osler stated that "Medicine is a science of uncertainty and an art of probability". There

This, in turn, empowers the development of AI-powered tools that can significantly impact patient care.

The integration of AI is driving a profound transformation across all levels of the healthcare sector. This integration enables advancements in disease prevention, treatment, and management. AI facilitates a deeper understanding of both individual and population health, leading to innovations that improve effectiveness and efficiency within healthcare delivery.

EU and its Member States are increasingly interested in integrating AI into healthcare. Their primary goal is to enhance the health of their citizens and deliver top-quality healthcare services. Moreover, they are facing a rising healthcare expenditure, which they hope to mitigate through efficient resource management made possible by digitization.

This explains the extraordinary momentum of AI in healthcare, which promises to introduce substantial changes that will take the digital transformation of the sector to the next level. Until now, digital healthcare (e-Health) was limited to the provision of remote healthcare services via the Internet (telemedicine) and the digitization of management (electronic medical records).[11] IA introduces a qualitative change that affects substantive issues and is transforming the practice of healthcare professions and the organization and management of healthcare services, leading to intelligent healthcare (i-Health).[12]

Although the transformative potential of AI extends to all sectors, it is essential to recognize that healthcare is a particularly sensitive area. Here it intersects with crucial legal values such as physical human life, privacy and human dignity. These values must be carefully balanced with the advancement of public and private activities. Consequently, intense public intervention has emerged aimed at safeguarding health and related principles and values while ensuring that healthcare delivery remains reliable and accessible.

In this context, the integration of AI into the healthcare sector is expanding across all its dimensions, with varied implications for the public interest and the rights and freedoms of citizens. These implications differ depending on the specific field in which AI is applied.

A distinction must be made between the use of AI in healthcare at the individual level and its professional application for healthcare purposes. In the first case, AI is used to monitor and improve health in the private sphere, both by citizens and companies, as evidenced by the proliferation of health apps in mobile devices (smartphones, smartwatches) that collect body data (Internet of Bodies, IoB). The management of a massive volume of citizens' health data, conveniently processed through AI systems, can contribute to the improvement of public health both at the individual level, promoting healthy habits and monitoring health status, and at the collective level, analyzing the health of the population, identifying problems or threats and allowing the planning and management of health strategies and policies in both the private and public spheres.

However, our focus here will be on the use of AI for healthcare purposes, which is governed by a complex legal framework comprising numerous overlapping and complementary rules. The applicable regulations vary depending on the scope and application of AI, thus necessitating the distinction and systematization of the various contexts in which AI can be employed within the healthcare setting:[13]

are innumerable reports from consulting firms that highlight the potential of AI in the field of healthcare, such as McKinsey Technology Trends Outlook 2022.

[11] Digital transformation for healthcare has so far been limited to so-called online government (e-Health), which essentially consists of putting healthcare online, as it is based in one specific technology, such as the Internet, and its sole purpose is to enhance interaction by eliminating the spatial and temporal barriers that separate healthcare services from patients. e-Health is purely instrumental, but not substantial, as it is limited to considering interactions between the healthcare systems and patients by streamlining information distribution and service provision, but without the ability to change the model or essence of healthcare. For an overview of e-Health see M.N. Moreno Vida, *Impacto de la medicina 4.0 en el sistema de salud*, in R*evista de derecho de la seguridad social. Laborum*, no. 6 (extra), 2024, 345-375.

[12] According to the characteristics of AI, digitalization will no longer be instrumental but substantive, as it affects decision-making and service-delivery processes. AI will lead to a real transformation of healthcare as detailed below.

[13] A summary in T. Davenport and R. Kalakota, *The potential for artificial intelligence in healthcare,* in *Future Healthcare Journal*, 2019, vol 6, no. 2, 2019, 94-98. Also see N. Terry, *Of Regulating Healthcare AI and Robots*, in *Yale Journal of Law and Technology*, no. 21, 2019, 3-20 and F.J. Estella Pérez and N. Escobedo Ortega, *La inteligencia artificial en el sector salud: aplicaciones e impacto*, in *I+S: Revista de la Sociedad Española de Informática y Salud*, no. 158, 2024, 21-24. A more detailed tour of the various applications can be found at *Artificial Intelligence in Healthcare: Applica-*

a) On the one hand, AI is playing an increasingly important role in research, becoming an indispensable factor in healthcare innovation. Thus, AI reduces the time and cost for the discovery of new drugs and makes it possible to identify new therapies for certain diseases.
b) In medical practice, AI systems find application across various segments of healthcare:
   1. Prevention: They enable the identification of future disease trends or health issues at both the individual and collective levels. For instance, software that forecasts cancer risk years in advance or detect suicide risk by analyzing behavior on social networks.
   2. Diagnosis: This is an area where significant progress has been achieved. For example, AI aids in diagnosing diabetic retinopathy from imaging or even COVID-19 from analyzing the sound of the voice.
   3. Treatment: AI is increasingly applied in treatments, ranging from precision surgery assisted by AI to personalized drug treatments or precision medicine.
   4. Patient Monitoring: AI systems are also utilized in monitoring patients, such as predicting epileptic seizures or assessing the success of rehabilitation for patients with addictions.
c) In healthcare management, AI software is increasingly used in the organization, management and delivery of healthcare services at different levels:
   1. Micro Level: AI systems optimize the scheduling of individual patient visits, enhancing efficiency in patient management.
   2. Middle Management Level: AI systems are employed for organizing services, including the coordination of urgent ambulance transport or the management of primary care services.
   3. Macro Level: AI systems play a role in structural decision-making within healthcare policies. This includes determining the locations of healthcare facilities, managing personnel policies, and making decisions regarding the authorization and financing of drugs.

As it can be seen, the use of AI systems occurs in very different domains, each presenting specific challenges and subject to distinct legal frameworks. Apart from these differences in the areas in which AI is used, two additional factors modulate the legal regime and implications of AI usage.

On the one hand, the role of AI systems in decision making must be taken into account. The implications are not the same when the AI system is used in an auxiliary way to support the decisions of healthcare professionals, and when they act in an automated way without direct human intervention in decision making.

Another relevant factor is the context of use of AI systems, whether it is the private sector or whether they are used by public institutions subject to additional obligations and guarantees such as Public Administrations.

3. *The European Union strategy for artificial intelligence in healthcare*

The significant potential presented by the integration of AI into healthcare systems, along with its strategic importance for the future of healthcare, has positioned it as a priority in EU's digital transformation policies. It is essential to recognize that the drive for the digital transformation of healthcare and the integration of AI into the EU stems from two distinct policies: digital policy and health policy.

Regarding digital policy, successive general strategies of the Union have increasingly emphasized the importance of AI, as evidenced in the current strategy outlined in the 2020 Communication "Shaping Europe's Digital Future," which includes generic mentions of AI. The 2021 Communication "Digital Compass 2030," goes further by establishing objectives for the incorporation of AI.[14] However, regarding the digitization of healthcare, these documents maintain a traditional perspective of e-Health, associating it primarily with the transition to electronic formats and

tions, risks, and ethical and societal impacts, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 729.512 – June 2022.

[14] The first reference to AI was included in the strategy "Shaping Europe's Digital Future" [Commission Communication COM(2020) 67 final, 19.2.2020] in which AI is mentioned generically as a relevant innovation and a White Paper is indicated as an action but without much pretension.
In the current strategy Digital Compass 2030: Europe's approach for the Digital Decade (Commission Communication COM(2021) 118 final 9.2.2021), references to AI are multiplied, although no specific section is dedicated to it, but reference is made to intelligent IT applications and a target is set for 75% of companies to have incorporated AI by 2030.

the implementation of telemedicine,[15] without providing specific references to the application of AI within healthcare.

On the other hand, European AI strategies have indeed recognized the healthcare sector as one of the most susceptible to transformation, and promoting AI in healthcare has been proposed as an objective.[16] However, this specific objective is not included in the European policy for Digital Administration, which maintains the traditional e-Health approach without explicit reference to the incorporation of AI.[17]

The Union's health policy is much more limited in scope, since it lacks competence over the organization and management of national health systems. Although there is no comprehensive EU health strategy as such, there has been a notable emphasis on digital-health initiatives. This involves primarily transitioning to electronic formats, with a strong focus on the significance of accessing health data to advance research, prevent diseases, and enhance personalized health and care.[18]

Indeed, it is within the Union's data policy where the most significant impetus for AI is indirectly occurring. Progress is being made towards establishing a genuine European health-data space, which serves as the fundamental basis for the operation of AI applications in healthcare.[19]

Beyond political directives, the EU's substantial drive for AI, specifically in healthcare, is evident through its funding programs.

The Union's long-term budgets and the NextGenerationEU recovery plan are dedicated to promoting a green and digital transition across all sectors, including healthcare. A substantial portion of the €750 billion allocated will be directed towards healthcare, facilitated through mechanisms established at the national level. This funding aims to enhance healthcare systems to better address future crises.

In addition to the Next Generation EU plan, the EU launched the EUproHealth 2021-2027[20] program in response to the COVID-19 pandemic, aiming to strengthen national health systems. With a budget of €5.3 billion, the EUproHealth program encompasses several action lines.[21] These include strengthening the use and reuse of health data for healthcare delivery and research and innovation, as well as encouraging the adoption of digital tools and services. Moreover, the program emphasizes the digital transformation of healthcare systems, which involves the integration of AI.

Indeed, it is evident that the Union is strongly dedicated to advancing the transformation towards digital healthcare. With a significant economic allocation, the Union aims to promote the digitalization of healthcare services, including integrating AI systems.

[15] The 2020 Communication "Shaping Europe's Digital Future" refers to the promotion of electronic health records, while the 2021 Communication "Digital Compass 2030" points to online interaction, paperless services, electronic transmission and access to data instead of paper and promotes access to digital health services.

[16] The Communication "Coordinated plan on artificial intelligence", 7 December 2018 [COM(2018) 795 final] pointed to this potential and prioritized the health-data space. For its part, the White Paper on Artificial Intelligence-A European approach aimed at excellence and trust, 19.2.2020 [COM(2020) 65 final] also highlights the transformation of AI in healthcare and, as established in action 6, promotes AI by the public sector and, as a priority, in healthcare.

[17] The Berlin Declaration on the digital society and value-based digital administration at the ministerial meeting during the German Presidency of the Council of the European Union on December 8, 2020 talks about improving health systems and medical care through interoperable digital solutions in the eHealth Network, such as the exchange of medical records or mobile health applications.

[18] On this issue see the Commission Communication on achieving the digital transformation of health and care services in the Digital Single Market; empowering citizens and creating a healthier society, COM(2018) 233 final, 25.4.2018. It makes hardly any mention of AI which is logical considering that at the time this technology was not yet too well known.

[19] The Communication "Towards a common European data space" COM(2018) 232 final of 15.4. 2018 containing the guidelines of the European data strategy pointed to the access and exchange of health data which is developed in the Communication on digital transformation of healthcare COM(2018) 233 final and leads to the proposal for a Regulation of the Parliament and the Commission on the on the European Health Data Space presented on May 3, 2022 and which will allow the massive exchange of health data at European level for both primary (medical use) and secondary (research) use that only make sense and prove useful because of their incorporation into AI systems.

[20] Regulation (EU) 2021/522 of the European Parliament and of the Council of 24 March 2021 establishing a program of Union action in the field of health ("EUproHealth program") for the period 2021-2027 and repealing Regulation (EU) 282/2014.

[21] The lines of action include improving and promoting health, protecting the population, providing access to medicines, health products and relevant products in the event of a crisis, ensuring that these products are available, accessible and affordable, and strengthening health systems.

4. *A map of the regulation of the artificial intelligence in healthcare within the European Union*

The current moment provides a favorable context for increased utilization of AI in healthcare at the European level. This calls for the urgent identification and systematization of the legal framework for AI in healthcare. Stakeholders, both public and private, in the sector are grappling with a complex web of regulations, including both existing laws and those pending approval. These regulations do not seamlessly align due to their differing bases, resulting in overlapping and disorderly arrangements.

As a starting point, it should be borne in mind that the European Union intervenes based on the principle of attribution of competences. Therefore, it is necessary to identify the competences through which it regulates the use of AI in healthcare.

On one hand, the Union holds competence over the single market, allowing it to intervene on AI as a "product". On the other hand, by virtue of this same competence over the single market, it can also regulate medical devices incorporating AI.

On the other hand, the Union has no competence to regulate the organization and management of national healthcare systems. It is therefore up to the Member States to regulate the use of AI in their healthcare systems taking into account the regulations on AI and medical devices.

Thus, the Union has a wide scope for action to regulate the use of AI in healthcare, but limited to AI as a technology and as a medical device – when used in medical practice –. On the other hand, its competence will be very limited when it comes to regulating how national healthcare systems should acquire, manage and use AI.

Taking into account the competencies of the Union, it is easier to systematize the regulations governing the use of AI in healthcare at the European level. It is useful to distinguish several blocks according to their purpose, which include specific rules on AI, healthcare-related rules applicable to AI systems and other general rules regulating the activity of these systems. The following sections analyze these regulatory blocks, outlined as follows:

a) A first block of specific measures on AI as a technology that includes both standards and soft-law measures:
   1. The Artificial Intelligence Regulation of 2024.
   2. The proposal for a Directive on liability for artificial intelligence.
   3. The European Declaration on Digital Rights and Principles for the Digital Decade 2023.
   4. The Ethical guidelines for trustworthy AI adopted by the Expert Group in 2019.
   5. Technical standards (ISO, IEC, CEN, CENELEC, ETSI, SIST).
b) The second block consists of health-sector regulations affecting the use of AI.
   1. Regulation of medical devices.
   2. National regulations on the organization and functioning of health systems.
c) The third block includes the general rules that apply to complementary issues that frame the use of AI in the healthcare setting:
   1. Data regulations.
   2. Regulations on digital services.
   3. Regulations on cybersecurity.
   4. Product safety regulations.
   5. Fundamental Rights.

4. *Artificial Intelligence Regulations that condition AI use in healthcare*

4.1. *European Union Regulation on artificial intelligence*

Among the specific regulations governing AI, the Regulation on Artificial Intelligence (RIA) takes center stage. Once approved in 2024, the RIA will not be fully applicable until two years after its entry into force. Nonetheless, it has already emerged as the cornerstone of regulating this new technology. It will serve as the pivotal framework that shapes the utilization of AI across all sectors, with particular significance in healthcare.

However, it is essential to note that the RIA does not provide a comprehensive and detailed regulation of AI as a technology. Instead, it focuses on setting specific restrictions of varying degrees depending on the particular use case. The regulation is based on the principle of freedom of use of AI systems, with limitations imposed only when there is an impact on rights, freedoms, and values. The primary objective of the RIA is to prevent fragmentation of the legal framework for AI by Member States that could impede free across-borders movement of goods and services

based on this technology.[22]

Therefore, the RIA sets forth a framework of minimum standards, including prohibitions and requirements, aimed at preventing harm that may arise from certain uses of AI. However, it also permits unrestricted development and use in all other cases. In essence, it serves as a foundational regulation that prohibits Member States from imposing additional prohibitions and requirements that may impede the free movement and use of AI systems.

This does not imply that there is no room for further development of the legal framework outlined in the RIA. Currently, it resembles more of a directive than a regulation, as it is crafted using a unique legislative technique that blends principle-based regulation with limited specific requirements. Additionally, it refers to further development through delegated and implementing acts by both the Commission and the Member States.

Furthermore, in addition to the general regulations on AI outlined in the RIA, sector-specific regulations will remain applicable. For instance, regulations on medical devices or the organization of healthcare systems may contain requirements that impact AI systems in those areas. This creates an additional regulatory framework that supplements the legal regime on AI, as will be further discussed in the following section.

The scope of application of the RIA is broad, encompassing a horizontal and comprehensive range that extends across the entire healthcare sector. Specifically, it includes all uses of AI within healthcare.

Specifically, concerning its objective dimension, the RIA encompasses all potential uses of AI systems across all sectors – with some exceptions[23] – regardless of whether their utilization is professional or private. This includes all AI systems utilized in healthcare, ranging from apps promoting healthy habits to those employed with medical purpose and for healthcare-service management.

Similarly, according the subjective dimension, the RIA applies to all entities involved in the development, deployment, and utilization of AI systems, whether individuals or legal entities, public or private.[24] This is particularly pertinent in the healthcare sector, as it implies that there is no differentiation based on whether the AI system is employed by private professionals or organizations or by the public health services of the Member States. Even if they are considered Public Administrations, they are not exempt from compliance with the RIA.

At this point, to understand how stakeholders in the healthcare sector fit into this framework, it is necessary to delineate the various parties bound by the RIA. The RIA distinguishes between providers – who develop an AI system or commission its development – and deployers, who professionally utilize an AI system under their authority. Lastly, there are the individuals affected by AI systems, known as the "persons concerned".[25] According to this configuration, healthcare professionals, companies, and organizations primarily fall into the category of deployers, as they typically do not develop AI systems but rather acquire them from vendors.[26] This distinction is significant because providers bear greater obligations, being responsible for ensuring the safety and reliability of AI systems as developers, while deployers are tasked with complying to the conditions of use. As for patients, they are the ones impacted by AI systems, benefiting from the security and assurance measures put in place, but their rights are relatively limited under the RIA.[27]

Finally, concerning the territorial dimen-

[22] Recital 1 states that the objective of the RIA is to improve the functioning of the internal market by laying down a uniform legal framework in particular for the development, the placing on the market, the putting into service and the use of AI systems in the Union, in accordance with Union value. Article 1 adds that the objective of the RIA is to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy AI, while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights.

[23] Certain uses related to transportation (art. 2.2) and to national security (art. 2.3) are excluded.

[24] "Provider" is defined as a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge; while the "deployer" a natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity.

[25] Article 3 of the definitions refers to all the parties involved, which are the provider, deployer, authorised representative, importer and distributor.

[26] In any case, to the extent that they can be considered to develop these AI systems – for example, by adapting an acquired AI system – they will be considered providers.

[27] Specifically, the right to an explanation of decisions taken individually (art. 86 RIA).

sion, it should be noted that the RIA applies to AI system-providers and deployer, regardless of whether they are established or located in third countries, as long as the output information generated by the AI system is utilized within the Union.[28] This extraterritorial reach of the RIA holds significance in digital activities, as they might be conducted from outside the Union but remain subject to its regulation.

The RIA sets forth prohibitions and requirements based on a risk-oriented approach that is open, proportionate, and adaptable, allowing for flexible intervention based on the level of risk posed by various AI uses. It delineates four risk levels: unacceptable-risk uses, which are prohibited; high-risk uses, subject to requirements verified through a conformity assessment; limited-risk uses, with minimum transparency obligations; and zero-risk uses, which are exempt from restrictions.

For systems intended for use in the healthcare sector, the classification as high-risk systems is particularly relevant, as they have a significant impact on public health, safety, and fundamental rights. AI systems are classified as high-risk in two main ways:

a) Firstly, high-risk AI systems include those utilized as safety components of products subject to conformity assessment under specific legislation, such as medical devices. Therefore, reference must be made to Regulation (EU) 2017/745, discussed below, to determine if an AI software can be considered a medical device. Among medical devices, those subject to a conformity assessment are classified as high-risk, while those subject to a declaration of conformity are excluded.
b) Secondly, all AI systems listed in Annex III of the RIA are considered high-risk. Among the systems listed that are relevant to healthcare are the following in order of importance:
    1. AI systems used to access public health services encompass all those involved in the management of health services.[29] This reference is particularly pertinent for AI systems not directly related to medical activities, as they are automatically classified as medical devices and thus deemed high-risk. Non-medical systems determining access to and utilization of health services, such as those scheduling medical appointments or calculating patient co-payments, fall into this category. Additionally, Annex III specifically mentions AI systems intended for assessing and categorizing emergency calls from individuals, as well as those utilized in dispatching or prioritizing first responders during emergency situations, including medical assistance services and emergency triage systems.
    2. Biometric identification systems utilized for biometric categorization[30] based on sensitive or protected attributes, such as race or ethnicity, represent another category, which may be used, for instance, in routine triage processes. Moreover, biometric identification systems employed for emotion recognition, serving purposes like identifying pain or addressing mental-health concerns, could be pertinent. If intended for medical applications, these systems would fall under the classification of high-risk medical devices and systems.
    3. Lastly, healthcare-provider companies and the national healthcare systems can use AI systems for personnel recruitment and decision-making processes concerning labor relations and performance evaluations that are also considered high-risk.[31]

    AI systems in Annex III will not be considered high-risk if they do not pose a significant risk of causing harm to the health, safety or fundamental rights of natural persons, especially when they do not substantially influence the outcome of decision making, i.e. when they are used as a complement to human decision making.[32] This exception does not

[28] As provided in Article 2.1 c).

[29] Annex III in paragraph 5(a) specifically refers to AI systems intended to be used by public authorities or on behalf of public authorities to evaluate the eligibility of natural persons for essential public-assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services.

[30] Included in Annex I, section I, which includes other cases.

[31] Annex III refers to them in paragraph 4 as an IA system for "employment, management of workers and access to self-employment".

[32] Article 6.3 RIA indicates that this is the case when the AI system is intended to perform a limited procedural task; improve the outcome of a previously performed human activity; detect patterns of decision making or deviations and is not intended to replace human evaluation; or when it performs a preparatory task for an eval-

apply to AI software for medical purposes, only to the AI system used in the management of healthcare benefits.

High-risk systems must meet a series of requirements, mainly subject to a risk-management system that allows them to be identified and analyzed, assessed and evaluated and subjected to the appropriate risk-management measures. In addition, there are other requirements related to data quality, documentation and traceability, transparency, human supervision, accuracy and robustness. Compliance with these requirements must be demonstrated by a conformity assessment conducted by an independent body designated by the Member States. Once the assessment has been passed, it is entered in a European register and the CE marking is affixed for placing on the market.

Furthermore, the RIA sets forth particular transparency requirements for AI systems designed to engage with individuals or to discern emotions, typically classified as limited-risk systems.[33] It mandates the disclosure of the use of an AI system in such interactions, as well as when employing emotion-recognition or biometric-categorization systems, which can be fulfilled through verbal notification or displaying a logo. This transparency mandate will impact numerous AI systems used in healthcare, particularly those involved in patient interactions, whether medically or administratively.

Apart from the mentioned cases, all other AI systems are free to use without any prohibition or requirement. However, these AI systems can voluntarily comply with the requirements applicable to high-risk systems through Codes of Conduct, even though they are not obligated to do so.

In healthcare, free-use AI systems will be less common, especially for medical purposes. Only those AI systems not considered high-risk, such as those not classified as medical devices or those subject to a declaration of conformity – not a conformity assessment –, will be available for free use. However, in health management, there may be a greater number of freely available systems, as only those directly impacting access to healthcare benefits will be considered high-risk.

uation relevant to the listed use cases.

[33] Article 50 RIA refers to transparency obligations of providers and users of certain AI systems.

5.2. *Other relevant artificial-intelligence Regulations*

In addition to the RIA, other European-level regulations on AI are emerging, with relevance to the utilization of AI systems in healthcare.

A case in point is the proposal for a Directive on AI liability, put forth by the Commission in September 2022.[34] The primary objective of this Directive is to harmonize certain national non-contractual fault-based liability rules, so as to ensure that persons claiming compensation for damage caused to them by an AI system enjoy a level of protection equivalent to that enjoyed by persons claiming compensation for damage caused without the involvement of an AI system. The Directive introduces two mechanisms aimed at overcoming this imbalance and facilitate tort-liability claims that may be frustrated by the complexity of AI systems and their opacity when dealing with black-box systems.

To this end, the Directive imposes the disclosure of evidence on high-risk AI systems to enable a claimant to substantiate a non-contractual fault-based claim for damages. Furthermore, it introduces a rebuttable presumption regarding the causal link between fault (failure of performance) and damage (system performance), thereby shifting the burden of proof in the case of non-contractual fault-based claims brought before national courts for damages caused by an AI system.[35]

It is, therefore, an initiative that will be absolutely essential to determine the patrimonial liability in the event of damage derived from IA systems in the healthcare field, making it easier for patients to claim against both healthcare providers and IA-system providers. In these cases, there seems to be no difference between a public or private healthcare provider, since, although the regulation refers to cases of civil liability, it is understood that this regulation is applicable to cases of liability of

[34] Proposal for a Directive of the European Parliament and the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive) COM(2022) 496 final, 28.09.2022. The liability of robots is a relevant issue see F. Ramón Fernández, *Inteligencia artificial y la atención médica: pacientes, diagnóstico y robots*, in *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, no. 56, 2022, 125-156.

[35] This is regulated in Article 4 of the proposed Directive, which refers to the rebuttable presumption of causality in case of fault.

administrations.[36] This however will be one of the issues to clarify.

Therefore, this initiative is crucial for finding liability in cases of damages caused by AI systems in healthcare, aiming to simplify the process for patients to seek compensation from both healthcare providers and AI-system developers. In these scenarios, the distinction between public and private healthcare providers seems negligible. While the regulation primarily focuses on civil-liability cases, its applicability to instances of administrative liability requires further clarification.

At present, the RIA (Regulatory Impact Assessment) and the proposed Directive on AI liability represent the EU's specific regulations concerning AI. However, it is likely that additional initiatives will arise at the European level, addressing specific facets, such as intellectual property. Moreover, sectors like transportation or national security, which are beyond the scope of the RIA, may also see dedicated regulatory efforts in the future. While it may seem logical to establish specific rules for the use of AI in sensitive sectors such as healthcare, the EU's approach is to apply a single general regulation, the RIA, to all AI applications. This does not preclude each Member State from applying its own regulations within its jurisdiction, including those relating to AI in sensitive sectors such as healthcare.

5.3. *Soft law on artificial intelligence*

The EU's strategy for governing AI goes beyond traditional regulation by incorporating various soft-law instruments to complement its legal framework.

A) Firstly, there are political documents recognizing digital rights, such as the European Declaration of Digital Rights and Principles for the Digital Decade, approved by the European Parliament, the Council, and the Commission on 23 January 2023. Chapter III addresses interactions with algorithms and AI systems, laying down principles applicable across various domains, including healthcare. These principles advocate for human-centered, reliable, ethical, transparent, and non-discriminatory AI systems. Moreover, they emphasize the importance of human oversight in AI-generated outcomes affecting people's safety and fundamental rights, cautioning against using AI to preempt decisions, particularly in healthcare.

While non-binding, these policy documents codify existing rights and indicate the emergence of new ones. They also serve as an interpretative criterion for existing regulations that may not yet fully encompass these principles.

B) Secondly, with the 2018 Ethical Guidelines for Trustworthy AI, established by the High-Level Expert Group, the European Union seeks to establish itself as a leader in promoting trustworthy and ethical AI practices.

While non-binding, these guidelines hold significant legal weight, serving as a reference for both the Union and its Member States in the development and interpretation of AI regulation. Additionally, they provide guidance for AI providers and users (deployers), outlining principles, requirements, and procedures for ensuring the reliability of AI systems.

C) A final important soft-law instrument with considerable influence is the standardization or technical normalization systems. These standards are not legally binding but are widely acknowledged by providers and users as benchmarks for quality and legal compliance. Due to their technical depth, detail, and adaptability, they effectively address the specifics left by mandatory hard-law regulations.

Notably, standardization is poised to play a crucial role, evident in the latest ICT Standardization Plans of the European Union,[37] which are paving the way for the development of the initial technical standards on AI.

[36] The term "civil liability" does not exclude the liability of the Administration. In addition, the proposal of Directive uses the RIA definitions of provider and user (deployer), which include both public and private parties. In addition, the explanation accompanying the proposal states that: "While this Directive does not apply with respect to criminal liability, it may be applicable with respect to state liability. State authorities are also covered by the provisions of the AI Act as subjects of the obligations prescribed therein."

[37] AI standards have been an important part of the successive EU Rolling Plan since 2018 and specific committees already exist (such as UNE Committee CTN 71/SC 42 Artificial Intelligence and Big Data) and specific standards have been adopted, such as: AI concepts and terminology (ISO/IEC 22989: 2022), biases in AI systems and AI-assisted decision making (ISO/IEC TR 24027:2021), guidelines for the implementation of AI systems (ISO/IEC 42001:2023), AI risk management (ISO/IEC 23894:2023).

6. *Health Regulations affecting the use of artificial intelligence*

6.1. *European Union Regulation on Medical Devices*

In addition to the general regulation on AI that conditions its uses, some sectoral regulations also affect the use of AI systems integrated in certain products and subject to specific regulations, such as toys, elevators, precision equipment, radio equipment and, as far as we are concerned here, medical devices that are subject to Regulation 2017/745 (EU).[38]

The definition of medical devices encompasses AI systems, as it expressly includes "software" intended by the manufacturer to be used by individuals for "specific medical purposes" such as:[39]

a) Diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
b) Diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
c) Investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
d) Providing information by means of in vitro examination of specimens derived from the human body.

Therefore, general-purpose software used within healthcare but lacking a medical purpose is excluded, as is software designed for wellness or lifestyle purposes.[40] The criterion is not whether the software directly impacts the human body, but rather whether its intended purpose aligns with that of a medical device.[41] Consequently, any software used for health services management unrelated to medical functions would also be excluded from being considered medical devices.

Finally, it should be noted that computer software can qualify as medical devices when it is used directly and independently, but also when used as an accessory when it serves to operate a medical device – for example, software that controls an insulin pump.

Medical-device software is categorized into different classes depending on the level of risk it poses to people's health. This classification dictates the extent of the requirements such products must meet before they can be commercialized, ranging from less stringent to more stringent standards.[42]

Thus, software intended to provide information for making decisions for therapeutic or diagnostic purposes is classified in class IIa, unless these decisions have an impact that could cause death or an irreversible deterioration of a person's state of health (in which case it would be class III), or a serious deterioration of a person's state of health or a surgical intervention (in which case it would be class IIb). On the other hand, software intended to monitor physiological processes is classified as class IIa, unless it is intended for monitoring vital physiological parameters, in which case it is classified in class IIb. All other software is classified as class I.

This classification of software as medical device responds to the classical programming paradigm, since they are limited to the typical functions of this type of software that complements – but does not replace – the activity of healthcare professionals, providing information for decision making or facilitating the observation of physiological processes. Therefore, automated medical-device software is

[38] Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC.

[39] Article 2 of Regulation (EU) 2017/745 which defines "medical device" as any instrument, device, equipment, hardware, software, implant, reagent, material or other article intended by the manufacturer to be used on humans, separately or in combination, for any of the following specific medical purposes. See S. Jabri, *Artificial Intelligence and Healthcare: Products and Procedures*, in *Regulating Artificial Intelligence*, in T. Wischmeyer and T. Rademacher (eds), Cham, Springer, 2020, 328-335.

[40] Recital 19 refers to general-purpose programs (e.g., a word processor used in a hospital) although the distinction is not so simple. It also leaves out computer programs aimed at wellness or lifestyle goals (such as health, sleep, diet, etc. apps) that do not have the status of a medical device.

[41] For an analysis of AI systems in medical devices in the United State see W. Nicholson Price II, *Artificial Intelligence in Health Care: Applications and Legal Issues*, in *SciTech Lawyer*, no. 14, 2017, 15-17. Also see N. Terry, *Of Regulating Healthcare AI and Robots*, in *Yale Journal of Law and Technology*, no. 21, 2019, 15-17. For an overview of the regulation of medical devices and a comparison between the EU and the USA see F. Pesapane, C. Volonté, M. Codari e*t al.*, *Artificial intelligence as a medical device in radiology: ethical and regulatory issues in Europe and the United States,* in *Insights Imaging*, vol. 9, 2018, 745-753.

[42] As provided in Rule 11 of Annex VIII of Regulation (EU) 2017/745. On the classification of AI software see A. Kiseleva, *AI as a Medical Device: Is It Enough to Ensure Performance Transparency and Accountability in Healthcare?,* in *European Pharmaceutical Law Review*, no. 1, 2020, 8-10.

not conceivable without direct human intervention, limiting the scope and potential of AI systems in medical practice.

All medical-device software needs a declaration of conformity – which is common to all classes – with which manufacturers guarantee that their products conform to the essential requirements. Depending on the classification, they must obtain a certificate of conformity – classes IIa, IIb, III and others – issued by a notified body that verifies the conformity of the products corresponding to different class requirements.

Regulation 2017/745 (EU) on Medical Devices and the RIA operate concurrently in the regulation of AI systems utilized for medical purposes. Their simultaneous application is not redundant, as each serves distinct objectives. The Medical Devices Regulation is primarily concerned with safeguarding health, whereas the RIA aims to protect other rights and interests of patients.[43]

Thus, AI systems that are considered medical devices will be classified, firstly, according to the classification of the Regulation on Medical Devices depending on the risk they pose to health. They are also classified through the RIA which, by default, classifies them as high-risk systems, regardless of the level of risk to health they pose.[44]

This implies that AI systems for medical purposes will have to undergo three conformity assessments: one based on their classification as medical devices and obtain a conformity-assessment certificate from a notified body at national level; one as high-risk AI systems from another notified body under the RIA; and an impact assessment, in cases involving high risks to the rights and freedoms of individuals under the RGPD data-protection regulation.

To avoid duplication and reduce burdens, the RIA integrates the supervision of the requirements relating to high-risk IA systems within sectoral regulations, resulting in a single conformity assessment that will be, in the case of medical software, the one applicable to medical devices.[45]

Although this solution is pragmatic, it has significant drawbacks. First, the criteria for evaluating AI systems – including transparency, impartiality, data integrity, traceability, oversight and robustness – are diluted within the sectoral procedure. This dilution occurs because the sectoral regulations primarily prioritize health protection, but do not fully address other values in the evaluation of AI systems. There is also a major organizational problem, as the incorporation of IA-system requirements into sectoral procedures exceeds the health expertise of the sectoral-assessment body, which will need to be restructured.[46]

6.2. *National Regulations governing Public Healthcare Systems*

Another sectoral regulation governing the use of AI in healthcare are the regulations of national public healthcare systems. In this re-

[43] Thus, the AI software with medical purpose ensures that it does not cause physical harm, but, in addition, that it does not affect privacy or equality. Recital 64 of the RIA highlights the different risks faced by the RIA with respect to sectoral regulation: "The hazards of AI systems covered by the requirements of this Regulation concern different aspects than the existing Union harmonisation legislation and therefore the requirements of this Regulation would complement the existing body of the Union harmonisation legislation. For example, machinery or medical devices products incorporating an AI system might present risks not addressed by the essential health and safety requirements set out in the relevant Union harmonised legislation, as that sectoral law does not deal with risks specific to AI systems."

[44] Therefore, an AI system for body temperature measurement will always be a high-risk AI system under the RIA, but may be classified as a Class I medical device which is the lowest level of risk.

[45] This is provided for in Article 74(4) RIA, which states that the supervisory procedures for IA systems do not apply when those legislative acts already provide for procedures ensuring an equivalent level of protection having the same objective. Recital 64 explains this solution: "This calls for a simultaneous and complementary application of the various legislative acts. To ensure consistency and to avoid an unnecessary administrative burden and unnecessary costs, providers of a product that contains one or more high-risk AI system, to which the requirements of this Regulation and of the Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation apply, should have flexibility with regard to operational decisions on how to ensure compliance of a product that contains one or more AI systems with all the applicable requirements of that Union harmonised legislation in an optimal manner. That flexibility could mean, for example a decision by the provider to integrate a part of the necessary testing and reporting processes, information and documentation required under this Regulation into already existing documentation and procedures required under existing Union harmonisation legislation based on the New Legislative Framework and listed in an annex to this Regulation. This should not, in any way, undermine the obligation of the provider to comply with all the applicable requirements". In a similar sense, see recital 81 with respect to quality-management systems.

[46] Thus, national authorities for the evaluation of medical devices will have to adapt in order to be able to verify the compliance of AI systems with the requirements related to aspects such as respect for the principles of equality, transparency, respect for fundamental rights, among others.

gard, it should be noted that the organization and management of public services is an exclusive competence of the Member States.[47] Additionally, since a significant portion of healthcare systems operate as public administrations, it is important to understand that the Union does not have competence over the organization and functioning of national administrations either.

Therefore, Member States have room to define the conditions for integrating AI systems into their healthcare system. This can be accomplished through regulations governing healthcare systems as well as through regulations governing the organization and operations of public administrations.

Member States must limit themselves to regulate the use of AI in the organization and management of healthcare systems. They should not interfere in matters relating to medical AI systems, as the Union's competence over the single market – exercised over both AI systems and medical devices – prevents Member States from adopting measures that would hinder the movement of these products.

To date, Member States have not enacted regulations specifically addressing the use of AI in healthcare systems.[48] This is likely because AI technology is not yet widely adopted, and there is anticipation for the European Regulation on AI, which is expected to establish the foundation and boundaries for any further national regulation. However, some Member States are taking steps by enacting measures on the use of AI in public administrations but more focused on their legal activity formalized in procedures, and less on the material provision of public services.[49]

7. *General Regulations framing the use of artificial intelligence*

The final regulatory block to consider encompasses general regulations that govern the use of AI. These regulations serve various purposes and do not specifically mention AI but nonetheless condition its use. They constitute the legal framework with which AI systems must comply and will be complemented, rather than replaced, by the RIA. It is useful to make a systematic list of all the regulations currently governing AI in healthcare. This list demonstrates that AI in healthcare is already regulated, even if not by specific regulations. Therefore, compliance with all these regulations is essential when using AI in healthcare, with the specific circumstances of each case determining the extent of its application.

Firstly, data regulations have increased significantly due to the European Data Strategy. This strategy is designed to maximize data potential and make their reuse and share easier within the market, while still protecting citizens' rights, especially their privacy. For this reason, the strategy relies on the General Data Protection Regulation, which will be applied whenever personal data are processed in AI operations.[50] Among the measures established to promote the free flow of data in the Union are the Open Data Directive, the 2022 Data Governance Act and the 2023 Data Act.[51]

[47] Article 168(1) TFEU provides that "7. Union action shall respect the responsibilities of the Member States for the definition of their health policy and for the organisation and delivery of health services and medical care. The responsibilities of the Member States shall include the management of health services and medical care and the allocation of the resources assigned to them."

[48] In Spain, the regulations that shape the National Health System, such as the General Health Act, the Cohesion and Quality Act and the regional regulations, contain provisions referring to digitalization – as in the case of the digital medical record or the electronic prescription –, but there are no specific provisions regarding AI.

[49] In the case of Spain, the provision applicable to the use of AI solutions by Administrations in general is Article 41 of 40/2015 Act on the Legal Regime of the Public Sector on "automated administrative actions" but it is not applicable to material activity as it is limited to actions taken in the framework of a procedure. On the other hand, Article 23 of Act 15/2022, on equal treatment and non-discrimination, which requires Administrations to promote mechanisms to ensure transparency, explainability, accountability and minimize biases in the algorithms involved in decision making; impact assessments following the principles set forth in the European Union regulations; and a seal of quality of the algorithm. In any case, there is no mandatory requirement, nor is it specified what these measures consist of, so that, in the end, it is a referral to the RIA. See J. Valero Torrijos, *The Legal Guarantees of Artificial Intelligence in Administrative Activity: Reflections and Contributions from the Viewpoint of Spanish Administrative Law and Good Administration Requirements,* in *European Review of Digital Administration & Law – Erdal*, 2020, vol. 1, issue 1-2, 55-61.

[50] On the application of automated decisions by AI systems in healthcare see J. Meszaros, J. Minari and I. Huys, *The future regulation of artificial intelligence systems in healthcare services and medical research in the European Union*, in *Frontiers in Genetics*, no. 13, 2022.

[51] The EU's data strategy is outlined in the Commission Communication "A European Data Strategy" COM(2020) 66 final, February 19, 2020. Within the data regulatory package are:
- General Data Protection: Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;
- Judicial Data Protection Directive: Directive (EU)

Furthermore, when AI systems are incorporated into online services, they fall under the scope of digital-services regulations. Specifically, this includes the Information Society Directive and the Digital Services Act when they are integrated into intermediary services such as online platforms and marketplaces. In addition, the Digital Markets Act applies to "gatekeepers," which are large-scale companies that operate key-platform services.[52]

Of particular relevance to the use of AI in healthcare are cybersecurity regulations. Among them, the NIS 2 Directive, which establishes measures for the coordination and management of security protocols for networks and information systems. Also, the Cybersecurity Regulation and the proposed Cybersecurity Products Regulation. In addition, the regulation on critical infrastructures affecting national health services.[53]

Furthermore, as AI systems are products, they are subject to general product-safety and product-liability regulations, including the General Product Safety Regulation and the Machinery Regulation, as well as to product-liability and general consumer and user regulations.[54]

Last but not least, AI systems will have to respect the system of fundamental rights, both those recognized at the European level in the Charter[55] and the European Convention on Human Rights, and those recognized at the national level in each of the Constitutions of the Member States.

This complete and dense set of rules applies to IA systems in general, regardless of their use. In any case, as these are generic rules, they are specified and/or displaced by the special rules that will be issued specifically on IA systems, namely the RIA and the proposed Directive on Liability on IA, to which other specific rules will be added.

8. *A critical overview of the European Union regulatory landscape of artificial intelligence in healthcare*

This review of the regulations governing AI in healthcare highlights the challenges posed by its regulation, as there is no specific regulation of its own, but rather different layers of rules regulating different aspects such as the use of AI, medical devices, national healthcare systems and multiple related aspects such as data, cybersecurity, etc.

In the case of Regulation on AI, it should be noted that although the RIA applies to all AI systems used in healthcare, it establishes requirements of varying intensity depending on the use in question. Thus, all AI systems used for medical purposes will be considered high-risk and must pass a conformity assessment. The same applies to AI systems used for healthcare management that affect the access

2016/680 of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data;
- Re-use Directive: Directive (EU) 2019/1024 on open data and re-use of public sector information;
Data Governance Act: Regulation (EU) 2022/868 of 30 May 2022 on European data governance;
- Data Act: Regulation (EU) 2023/2854 of the Council of 13 December 2023 on harmonised rules on fair access to and use of data.

[52] The Digital Services Package contains the following legislation:
- Directive on electronic commerce: Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market;
- Digital Services Act: Regulation (EU) 2022/2065 of the Council of 19 October 2022 on a Single Market For Digital Services;
- Digital Markets Act: Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector.

[53] Cybersecurity regulation applicable to AI systems include:
- NIS Directive 2: Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union;
- Cybersecurity Act: Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification;
- Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements COM/2022/454 final;
- Critical Infrastructure Directive: Directive (EU) 2022/2557 of 14 December 2022 on the resilience of critical entities.

[54] Product and consumer-protection regulations include:
Consumer protection Regulation: Regulation (EU) 2017/2394 of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
- Product Safety Regulation: Regulation (EU) 2023/988 of the Council of 10 May 2023 on general product safety;
- Machinery Regulation: Regulation (EU) 2023/1230 of the Council of 14 June 2023 on machinery;
- Proposal for a Directive on liability for defective products COM/2022/495 final;
- Consumer Protection Regulation: Regulation (EU) 2017/2394 of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[55] Charter of Fundamental Rights of the European Union of 2000 (2016/C 202/02).

to healthcare benefits. Otherwise, all systems that interact with people or recognize sentiments will be subject to transparency obligations. All other AI systems used in healthcare are free to use and will not be subject to any limitations or requirements.

As for the Regulation on medical devices, it covers a large part of the AI systems used in healthcare since it applies to all those AI-products that have a specific medical purpose – diagnosis, prevention, monitoring, prediction, prognosis, treatment or disease alleviation – and will be classified according to the risk they present to health, so they must, in all cases, make a declaration of conformity, and in cases of greater risk to health they must obtain a conformity assessment.

The national regulations on the organization and operation of public health services can specify how AI systems can be used into the public system in terms of access to health benefits. The problem is that it can lead to two modes of AI use by establishing unjustifiable differences between use of AI in public healthcare, which would be subject to stricter rules, and the use of AI in private healthcare, which would be subject to general requirements.

Finally, there are the numerous general data, digital services, cybersecurity, consumer and fundamental rights regulations to comply with, in addition to AI and medical device-specific regulations that may modulate or shift their content.

The unique structure of the legal framework regulating AI in healthcare suggests that it may be insufficient due to the lack of specific legislation tailored to this context.[56] While measures such as the RIA, together with the proposed Directive on AI liability and soft-law measures, help mitigate the risks associated with AI systems in healthcare, they do not fully address the risks associated with their medical use. Conversely, the Regulation on Medical Devices ensures the safety of AI systems for medical purposes, but does not cover other non-health-related aspects, such as equality, transparency, etc.

Therefore, it is crucial that all these regulations are applied in a complementary and coordinated manner to ensure effectiveness without imposing excessive burdens on individuals. Without proper coordination, an AI system intended for medical use might need to undergo multiple conformity assessments, including those for medical devices, high-risk AI, and data protection. Hence, the RIA, in the case of AI software considered to be medical devices, refers to sectoral assessment procedures, although this solution is questionable due to the lack of specialization of the body that must carry out this assessment.

Moreover, the Regulation on medical device may be outdated to cope with the peculiarities of AI systems, as they were developed to ensure the safety of classical programming software with medical purpose. This raises difficulties, on the one hand, for the classification of AI systems as medical devices, since many of them are used as decision-support systems and, although the CJEU has adopted a functional criterion in the definition of medical devices based on medical purpose, this may be difficult to apply in some cases. On the other hand, the use of AI systems in healthcare also poses problems, since their autonomous software is not allowed and no reference is made to the relevance that these systems can have in decision-making, which, in some cases, can even replace them.

These shortcomings highlight the importance of adopting a strategy regarding the use of AI in healthcare. The European Parliament has proposed some alternatives[57] such as:

a) Extend AI regulatory frameworks and codes of practice to address healthcare-specific risks and requirements; Promote multi-stakeholder engagement and co-creation throughout the whole lifecycle of medical AI algorithms;
b) Create an AI passport and traceability mechanisms for enhanced transparency and trust in medical AI;
c) Develop frameworks to better define accountability and monitor responsibilities in medical AI;
d) Introduce education programmes to enhance the skills of healthcare professionals and the literacy of the general public.
e) Promote further research on clinical, ethical and technical robustness in medical AI;
f) Implement a strategy for reducing the European divide in medical AI.

[56] For a similar critic see H. van Kolfschooten, *EU Regulation of Artificial Intelligence: Challenges for Patients' Rights*, in *Common Market Law Review*, no. 59, 2022, 81-112.

[57] See *Artificial Intelligence in Healthcare: Applications, risks, and ethical and societal impacts*, EPRS | European Parliamentary Research Service, Scientific Foresight Unit (STOA) PE 729.512 – June 2022, 46-53.

The most straightforward solution may be the enactment of specific regulation at the European level to address the unique characteristics of AI systems in healthcare. Such regulations should integrate the requirements outlined in the RIA and update those of the Regulation on Medical Devices. The growing relevance of AI systems in healthcare and their profound impact makes it advisable to adopt a comprehensive regulation to ensure the safe and responsible use of these technologies in such a critical and sensitive area as healthcare, which involves numerous rights, health and human life.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 49-55
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 05

*e-Transformation in the Polish Healthcare System. Data in Healthcare Entities**

Paulina Gruszka
(Higher Vocational Education School in Wrocław)

Małgorzata Kozłowska
(Research Fellow at the Institute of Administrative Sciences, Department of Administrative Law, Wrocław University)

ABSTRACT This publication aims to familiarise the reader with the digital transformation that has taken place in the Polish health care system; To draw attention to the category of data processed as part of the "e-Health" phenomenon, as well as their role in the system. To describe to the reader the basic legal and organisational solutions for the processing of medical data in the health care system.

1. *Introduction, or some remarks on the digital transformation in the Polish health care system*

Health care is an important task of every modern state, being part of the so-called prestative administration. For this reason, the provision of health care services either directly by the state or, as part of gradual privatisation, by private entities equipped with public funds, is widely accepted. There is also no doubt that the implementation of public tasks in the field of health care and their supply should be carried out according to certain values, among which the compliance with the principles of: quality and safety, equal access to the system and continuity of health services are crucial.

Health services - as a result of the transformation of society into an information society - are increasingly taking the form of services provided electronically,[1] i.e. with the use of information and communication technologies (ICT). According to the Polish Act of 18 July 2002 on provision of services by electronic means,[2] implementing Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 - a service provided by electronic means is a service which: 1) is provided at a distance, 2) via electronic processing equipment, 3) at the request of the recipient of the service and 4) for remuneration.[3] The phenomenon of electronically delivered medical services is referred to as: telemedicine, teleconsultation, sometimes a general term appears in their context, i.e. "e-Health", although these are not synonymous terms. Without entering into detailed discussions in this regard, it is only necessary to point out that the term "telemedicine" refers to activities directly aimed at achieving a therapeutic objective, including in its scope: prophylaxis, diagnosis, treatment and control of patient's state of health, carried out with the use of means of distance communication. The Polish legislator does not introduce a legal definition of the notion of 'telemedicine', however, it allows for the possibility of providing medical services by means of teleinformation systems or communication systems.[4] In such an

*Article submitted to double-blind peer review.

[1] The literature points out that due to the Community nature of the concept of 'information society service', it is not uniformly transposed by national legislators, e.g. the Polish legislator uses the concept of 'electronically provided service'. On this subject: I. Wrobel, *Pojecie usługi społeczeństwa informacyjnego w prawie wspólnotowym*, in *Cbke e–biuletyn,* no. 4, 2007, https://www.bibliotekacyfrowa.pl/Content/22509/PDF/Pojecie_uslugi_spoleczenstwa_informacyjnego.pdf.

[2] Single uniform text in Journal of Laws 2020 of 3 March 2020.

[3] Although the Polish legislator does not introduce the premise of remuneration, it is present in the provisions of EU law, in particular in Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services, as amended by Directive 98/48/EC. According to the case law of the CJEU - the premise of remuneration does not imply a requirement for the person who uses the service to pay for it, the economic dimension of the service in question is important.

[4] Article 3(1) of the Act of 15 April 2011 on therapeutic activity, (single uniform text in Journal of Laws 2022.633 of 2022.03.18).

approach, the notion of 'telemedicine' is similar to the notion of 'teleconsultation', which, regulated and named in the Polish national law, means precisely health services provided at a distance with the use of tele-information systems or communication systems.[5] Thus, telemedicine or teleconsultation services should be referred to services which have the nature of health services. On the other hand, the notion of 'e-Health' is broader than the notion of 'telemedicine' and 'teleconsultation' and, apart from actions aimed directly at achieving a therapeutic goal, also includes accompanying services consisting in: processing of data about the patient's state of health, maintaining electronic medical records, issuing e-prescriptions, e-referrals and e-medical leave, the broadcasting of medical procedures for students or e-learning services in general. However, according to some doctrinal positions, not all e-Health services can be qualified as information society services, e.g. a simple teleconsultation consisting of an exchange of information and experience between medical specialists will not have such a character.[6] On the basis of the analysis of the normative material and the jurisprudence of the CJEU - a certain line of demarcation in this regard may be the assessment whether the "e-Health" services are inextricably linked to the relevant telemedicine or teleconsultation service, and if the answer is in the affirmative, it is possible to qualify the e-ealth service as an information society service.[7]

Providing health services by electronic means in the Polish health care system - being an innovative form of providing medical care - is increasing, also under the influence of experiences related to the SARS-CoV-2 virus pandemic. Some of these services - taking into account previous findings - will have the hallmark of information society services, while others, which will not be inseparable from the provision of health services, will be part of the broadly understood e-Health phenomenon, (e.g. a medical examination or a procedure performed in the doctor's office with the physical presence of the patient with the use of electronic equipment). The purvey of health services via electronic means results in a win-win situation for the patient, which of course is not without some associated risks. Among the advantages of telemedicine is that it facilitates access to specialists, not only for groups subject to social exclusion (e.g. inhabitants of rural areas and small towns), as is generally assumed, but also in situations where, due to the high level of complexity of a specific case, it becomes necessary to conduct a meeting with a wider group of specialists (e - procedure, e - surgery). The literature emphasises that the benefits of well-integrated ICT tools, such as lower costs and health safety for patients, include preventing or postponing the placement of patients in inpatient care, which is costly and sometimes even ineffective from the perspective of the patient's recovery.[8]

Information and communication technologies (ICT) can be used directly for patient health care, in particular when they mediate a visit (so-called e-visit), or when a patient, e.g. after hospitalisation or with a chronic illness, requires continuous monitoring of his or her health condition (e.g. with the help of an e - ECG, e - ultrasound or e - stethoscope) together with the assessment of parameters by a medical specialist at any time. It is also necessary to take into account such solutions that indirectly contribute to the protection of individual health, the axis of which will be preventive and educational activities, i.e. those consisting in e - instruction, e - rehabilitation and e - prophylaxis. Going one step further, it is worth pointing to solutions in the field of video monitoring applied to persons with intellectual disabilities or senile dementia, which are intended to protect the above-mentioned categories of persons from the

[5] The concept of teleconsultation is regulated in the Regulation of the Minister of Health of 12 August 2020 on the organisational standard for teleconsultation in primary healthcare (uniform text in Journal of Laws 2022.1194 of 2022.06.06).

[6] D. Gęsicka, *Pojęcia „usługi telemedycyny", „tel-emedycyna", „e-zdrowie"* in I. Lipowicz, G. Szpor and M. Świerczyński (eds.), *Telemedycyna i e-Zdrowie. Prawo i informatyka*, Warsaw, 2019.

[7] In this context, attention may be drawn to motive 18 of Directive 2000/31/EC, according to which the notion of information society services encompasses a wide range of activities carried out on line and includes both services providing the opportunity to conclude contracts on line and services offering information and commercial services; ECJ judgment of 4.05.2017, C-339/15, Criminal proceedings against Luc Vanderborght, ZOTSiS 2017, no. 5, item I-335.

[8] See I. Lipowicz, *Administracja świadcząca na odległość – Nowe wyzwania administracyjnoprawne*, in I. Lipowicz, G. Szpor and M. Świerczyński (eds.), *Telemedycyna i e-Zdrowie. Prawo i informatyka*, Warsaw, 2019.

dangers of damaging their health or even loss of life. It should also be kept in mind that, despite the increase in areas where telemedicine can be used effectively, it cannot be treated as an alternative to traditional forms of treatment. Therefore, in some cases, it will not find justifiable use (e.g. when - for reasons of the patient's state of health, treatment and prognosis - services performed in the direct presence of the patient are necessary). This distinction is illustrated in the figure below.

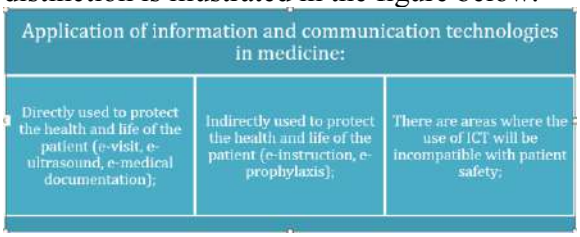


Figure 1: Application of information and communication technology in medicine

Thus, to summarise the previous considerations - health services provided via ICT means, i.e. telemedical services, can be effectively provided in the Polish health care system. It should be borne in mind that telemedicine benefits should correspond to the same level of professional requirements - which are appropriate for traditional health insurance benefits, of course taking into account the specificity of telemedicine services. The provision of telemedicine services - as previously agreed - is possible if: this is in accordance with the requirements of current medical knowledge and with the principles of professional ethics, the supply of these services does not conflict with legal regulations and - as will be discussed later - all requirements for the security of data processing are met.[9]

The use of information and communication technologies in health care requires the development and implementation of a system capable of sharing information, i.e. an interoperable system. Such a system should take into account the needs of patients. It should be directed towards secure access, exchange and use of electronic health information, through patient websites, using mobile applications and artificial intelligence. Such systems should also meet requirements to ensure the integrity of the content and data contained therein, permanent access for authorised persons and access control. In the Polish healthcare system, as part of ensuring interoperability of the healthcare system, a solution has been implemented that consists of the use of electronic document templates in a standard allowing for the inclusion of strictly defined data and the exchange of this data between individual systems used in the medical environment, The templates discussed here are part of a globally used standard - HL7 (Health Level Seven). The use of ICT tools or other medical devices also requires the creation of a range of organisational arrangements that make the solutions discussed here accessible to users. Moreover, due to the fact that the consequence of e-Health involves the removal of natural barriers protecting privacy, and the subject is the circulation of data, especially personal data, including sensitive data concerning the patient's state of health, it is necessary to design legal and organisational resolutions, and then to implement them correctly, in a manner which will guarantee the security of data and will express concern for the well-being, privacy and safety of the patient, i.e. - the beneficiary of the health care system.

The change that has taken place in the Polish health care system as a result of the use of ICT is significant. The analysis of the basic solutions in this area makes it possible to distinguish certain areas in which ICT solutions are used. First of all, we can distinguish the area of telemedicine in general, which - referring to the previous findings - consists in providing health services at a distance. Within this area, attention should be paid to e-medical leave, e-prescriptions and e-referrals embedded in the system, as well as solutions in the field of diagnostics, treatment and prevention of certain diseases (e.g. cardiovascular and respiratory diseases). Another area in which ICT solutions are used is medical documentation. The Polish regulation in this area establishes as a rule the keeping of medical records - in electronic form.[10] Another significant area using ICT is the flow of medical data and archiving (Internet Patient Account). In this context, it

[9] *Jak skutecznie wykorzystać potencjał telemedycyny w polskim systemie ochrony zdrowia?*, Warsaw, 2018, 36, report prepared for the Telemedicine Working Group Foundation, available on the website: http://telemedycynaraport.pl/api/file/events/rtgr/DZP_raportTGR%20raport-www.pdf.

[10] Regulation of the Minister of Health of 6 April 2020 on types, scope and models of medical records and the manner of their processing (single uniform text in Journal of Laws 2022.1304 of 2022.06.22).

should be noted that the diagnostic and therapeutic process depends to a large extent on the exchange of information between units of the system. The flow of medical data via IT systems undoubtedly improves the diagnostic and treatment process. Finally, one can mention the area of promoting research and development activities and entrepreneurship in the field of e-Health. The Polish legislator has also recognised the need to implement IT tools in the area of collecting data on adverse events and the occurrence of potential non-compliance in the practice of a healthcare entity.

Some telemedicine or e-Health solutions take the shape of pilot programmes, the aim of which is to identify the basic barriers to implementation and to gather knowledge on the functioning of a given solution, its evaluation and possible correction. Currently, in Poland, the project evaluates, among other things: the usefulness of using ECG patches to remotely monitor a patient's health condition, and the usefulness of using e - spirometers and e - stethoscopes for post-covid prophylaxis. An e - registration scheme is also being implemented, assessing the effectiveness of patient queue management using an algorithm.

2. *Data in healthcare entities*

An element of the purvey of healthcare services as information society services, among others, is the processing and storage of data.[11] Thus, the widespread use of efficient ICT systems implies the creation and functioning of various databases and medical registers.[12] In the health care system, data are processed that are necessary for the public health policy, for improving the quality and availability of services and for health care tasks to be cost-effective. Accordingly, data in the health system is data that is collected not only by healthcare entities as part of their actual activities, but also as a result of collection from various measuring and diagnostic devices, brought in by patients and cooperation with various other entities of the system.[13] Thus, the data collected in the health system can be diverse and serve different purposes. We can speak of statistical, financial, structural or qualitative data. Therefore, it can be hypothesised that data lies at the heart of an organised health system. In other words, the more the health system wants to meet the demands placed on it and respond to the needs of its stakeholders, the more attention it must pay to the collection and gathering of adequate, high-quality data[14] and its proper analysis. The variety of data in the health system is presented in the figure below.

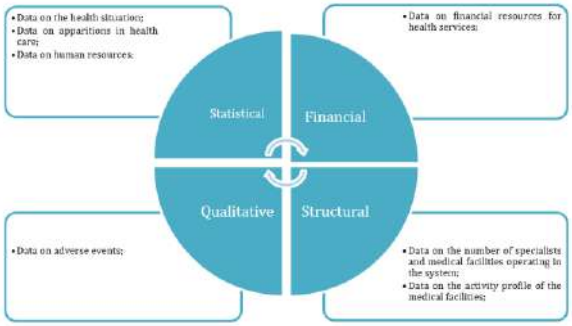


Figure 2: Types of data collected in the health system

Data processing in the health system has a variety of undertows, and is carried out under different legal titles. Among the many categories of data commonly collected in the health care system, those containing information about individuals occupy a special category.

3. *Medical data as a special category of data*

The processing of personal data in healthcare entities includes a variety of activities related to patient data, which may consist of: the collection of information during patient registration - both conducted in traditional form and using ICT tools; consultation with a specialist, including through telemedicine or teleconsultation; the completion of medical records in an ICT system; the exchange of information about a patient's health status; sometimes the transfer of data to other country, as well as the storage of medical records and their deletion. The source of these data can be either - a human being, i.e. a healthcare professional, or the entire organised infrastructure for the provision of a specific healthcare service. With reference to the previous adjudications, it should be recalled that

[11] M. Podleś, in J. Gołaczyńskiego (ed.), *Umowy elektroniczne w obrocie gospodarczym*, Warsaw, Difin, 2005, 251.

[12] By way of example only, the following medical registers can be mentioned: Register of Medicinal Products; Register of Medical Assistants; Register of Pharmacies; Register of Healthcare Providers.

[13] K. Wojsyk, *2. Jakość danych związanych z lokalizacją w przestrzeni*, in I. Lipowicz, G. Szpor and M. Świerczyński (eds.), *Telemedycyna i e-Zdrowie. Prawo i informatyka*, Warsaw, Wolters Kluwer, 2019.

[14] High-quality data is data from a reliable source, verifiable, unambiguous, identifiable.

the consequence of the supply of health services through information and communication means is the processing of data in an electronic environment, which leads to an intrusion into the privacy of the patient. The data processing is necessary for the fulfilment of the database administrator's legal obligation, while it is beneficial for the patient. For this reason, health is combined with an interference with another issue - privacy. Because the activities for the protection of health of an individual cannot override his/her right to privacy - it became necessary to develop legal means and to determine the conditions under which the personal data of a patient will be processed.

Patient's data is a special category of data, the so-called sensitive data, which determines their special protection (as their processing may cause risk for the data subjects) and certain obligations of medical entities providing health services in this respect. These obligations - as rightly noted by the representatives of the doctrine - should aim at securing personal data and consist in the implementation of adequate technical and organisational solutions which are to enable safe and lawful processing of personal data of individuals, including persons using the services offered by the healthcare entities.[15] The detailed manner of handling the data in question here and the relevant obligations of healthcare entities are normalized in particular - common to all Member States - by the EU Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR),[16] which regulates the most important issues in this regard, and by the national regulations adopted in the Member States, which are sometimes complementary.[17] The aforementioned regulations formulate as their objective - the protection of data subjects from the negative consequences of the processing operations, which is why the above-mentioned regulations indicate, in particular, the rights of data subjects and define the specific obligations of database administrators and other processing entities (so-called processors), which process the data of natural persons in an automated manner.

A patient's personal health data is information that concerns the physical and mental health of an identified or identifiable natural person. It is worth emphasising that the mere possibility of identifying a person, through the association of information, makes the information personal data. The identification of a patient can be made on the basis of: first name, surname, PESEL number, international classification of diseases (ICD-11), internet identifier and many other characteristics. It is also worth emphasising that certain health data - due to anonymisation - will not be subject to the GDPR regulations (e.g. statistical data).

Among the sensitive data protected, the GDPR includes – "all data about the health status of the data subject revealing information about the past, present or future physical or mental health of the person". The GDPR specifies that this will include, but is not limited to: information collected during registration and during the provision of healthcare services; information from laboratory tests or medical examinations; information about the disease, disability, disease risk, medical history, clinical treatment and physiological or biological state of the data subject.[18] Nevertheless, it should be kept in mind that the information listed in the GDPR, which constitutes a category of personal data of the patient, is only of illustrative, interpretative value, as the scope of the data is in fact broader.

The Data Protection Regulation in Article 9(1) formulates a general prohibition on the processing of sensitive data, including data relating to health, however, healthcare providers may process patient data on the basis of Article 9(2)(h) - for the purposes of preventive health or occupational medicine, for the assessment of a worker's fitness for work, medical diagnosis, the provision of healthcare or social security, treatment or the management of healthcare or social security systems and services on the basis of EU law, Member State

[15] P. Fajgielski, *Prawo ochrony danych osobowych Zarys wykładu*, Warsaw, 2019, 20.

[16] Journal of Laws UE.L.2016.119.1 of 2016.05.04, GDPR.

[17] These will be legal regulations of various types and ranks, ranging from constitutional provisions, international and EU law, national laws and implementing acts; The national regulation that serves the application of the GDPR - is the Act of 10 May 2018 on the protection of personal data (uniform text in Journal of Laws 2019.1781 of 2019.09.19).

[18] The legal definition of health data can be found in Article 4 para. 15 of the GDPR, it is complemented by motive 35 of the GDPR preamble.

law or in accordance with a healthcare professional subject to the conditions and safeguards referred to in Article 9(3) GDPR. In addition, under Article 9(2)(i), it is possible to process data when this is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border health threats or ensuring high standards of quality and safety of healthcare and medicinal products or medical devices, on the basis of EU or Member State law, which provides for appropriate specific measures to protect the rights and freedoms of data subjects, in particular professional secrecy.

Healthcare institutions processing sensitive data (database administrators) have been obliged to secure such data by implementing adequate technical and organisational solutions to enable the safe and lawful processing of personal medical data. At the same time, the GDPR does not explicitly formulate specific technical and organisational conditions, it only indicates in Article 32 - system features and functionality, which is probably dictated by the fact that the processing of personal data takes place in the face of constant technological progress.[19]

Medical entities not only process, but also transfer - on the basis of contracts, by law, or on specific request - the patient's medical data to other entities, organisations and institutions operating in the health care system (e.g. other medical specialists) and public authorities (National Health Fund (payer), control and supervisory bodies). In case the healthcare entity (administrator) transfers the data to other entities, institutions and organisations on the basis of the personal data processing entrustment agreement (processor) - it is obliged to choose the processing entity which provides the guarantee of implementation of appropriate technical and organisational measures which are to ensure lawful and secure processing for the data subjects. When entering into a processor entrustment agreement, the administrator must ensure that it complies with the requirements set out in Article 28 GDPR. In practice - the administrator (healthcare provider), before entering into an entrustment agreement, should verify that the processor, inter alia: already processes health data or other sensitive data; has appointed a Data Protection Officer; has implemented technical and organisational measures that will protect the rights of data subjects; has carried out a data protection impact assessment; has implemented procedures for security incident management; undergoes regular data security audits; ensures that persons authorised to process data are bound by confidentiality agreement; and has joined a code of conduct or certification mechanism.[20]

4. *Protection of patient medical data under the GDPR*

Patient information as sensitive data is subject to special legal protection. This applies to medical data as well as other data, such as identification or contact data. Ensuring the appropriate level of this data - as mentioned above - is particularly important when providing telemedicine services. For this reason, administrators - or other processors - are obliged to secure these data by implementing adequate technical and organisational solutions to enable safe and lawful processing of the patient's personal data. The administrator is furthermore obliged to implement the rights of data subjects, among which - according to the GDPR - are: The right of access to personal data; the right to rectification of personal data; the right to be forgotten; the right to restrict the processing of personal data; the right to data portability; and the right to object. The exercise of some of these rights may be limited due to national law (e.g. the right to erasure of data contained in medical records cannot be exercised before the expiry of the statutory retention period). The protection of patients against the negative consequences of unlawful data processing takes into account the application of measures of a preventive nature (consisting precisely in determining the principles of data processing and the obligations of administrators and processors) and repressive measures (e.g. administrative fines).

5. *Conclusion*

The use of information and communication tools in health care brings a number of benefits to all participants of the health care sys-

[19] On this topic, among others: B. Marcinkowski, *3.3. RODO*, in I. Lipowicz, G. Szpor and M. Świerczyński (eds.), *Telemedycyna i e-Zdrowie. Prawo i informatyka*, Warsaw, Wolters Kluwer, 2019.

[20] *Jak skutecznie wykorzystać potencjał telemedycyny w polskim systemie ochrony zdrowia?,*Warsaw, 2018, 89, report prepared for the Telemedicine Working Group Foundation, available on the website: http://telemedycynaraport.pl/api/file/events/rtgr/DZP_raportTGR%20raport-www.pdf.

tem. Telemedicine - as a complementary form - in relation to the classic form of providing services allows to respond to some of the needs of an ageing society. Thanks to the use of telemedicine solutions, the effectiveness of telemedically delivered health services is steadily increasing. The widespread use of telemedicine solutions is supported at European Union level, which, in the context of a mobile society, is to be welcomed.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 57-69
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 06

*Liability of the Spanish Health Administration for the Use of Artificial Intelligence**

Juan José Mantilla Sandoval
(Researcher at Carlos III University of Madrid – Legal Director at Dentons Paz & Horowitz)

ABSTRACT The development of disruptive technologies such as artificial intelligence undoubtedly facilitates various human activities, but requires enormous efforts from legislative institutions to regulate these technologies in a way that guarantees the protection of people's rights without hindering innovation. This paper, by analyzing each of the requirements identified by the Spanish judicial bodies for the determination of liability against the Public Administrations, demonstrates precisely the need to update this regime, specifically in the field of public health, since it is not designed to be applied to damages caused by artificial intelligence. In addition, this analysis contributes to the identification of certain key aspects that must be considered when designing a specific regulation under European Union directives and guidelines.

1. *Introduction*

The history of mankind has been characterized by constant technological development, facilitating the execution of all types of activities, and improving living conditions. During the last three centuries, it is possible to identify four industrial revolutions that have defined progress for mankind.

The First Industrial Revolution, tied to the invention of the steam engine and the development of railroads, considerably facilitated mass transportation of materials and people. The Second Industrial Revolution was defined by electricity and the implementation of the assembly line in mass production. The Third Industrial Revolution yielded the widespread use of electronics, the invention of computers and the use of digital-information technology to automate production and facilitate communication on a global scale. And finally, the Fourth Industrial Revolution is ongoing and is characterized by the implementation of nanotechnology, robotics, biotechnology and, above all, artificial intelligence, which has allowed for an exponential increase in the capacity to store and process information, with smaller margins of error than the ones achieved by the cognitive capacities of humans.[1]

The enormous advantages generated by technological development are unquestionable. For example, artificial intelligence has created machines capable not only of processing a greater amount of data and at greater speed than human beings, but also of executing actions with greater precision and effectiveness.

Without undermining these obvious advantages, these types of technologies have recently confronted mankind with enormous challenges. People are now exposed to new, previously unsuspected risks with very significant ramifications in the legal sphere.[2] It is no coincidence that the adoption of each technological invention, and the transition to a new industrial revolution, has been followed by the enactment of appropriate regulatory frameworks. Such are the examples for frameworks regarding terrestrial and aerial transportation, electric power, oil exploitation, cybersecurity, privacy, etc. These efforts have marked the history of mankind, evidencing the perpetual pursuit between law and human development. This pursuit has even accelerated with the Third and Fourth Industrial Revolutions, where humanity has been exposed to the so-called risks of digital freedom, creating situations where a large

*Article submitted to double-blind peer review.
This work has been carried out as part of the research project "The impact of artificial intelligence in public services: a legal analysis of its scope and consequences in healthcare" (PGC2018-098243-B-I00) which is developed under the direction of Professor José Vida Fernández within the 2018 Announcement for "Knowledge Generation R&D Projects" issued under the State Program for Knowledge Generation and Scientific and Technological Strengthening of the R&D System promoted by the Spanish Ministry of Science and Innovation.

[1] J.G. Corvalán, *Inteligencia Artificial: retos, desafíos y oportunidades – Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la justicia*, in *Revista de Investigaciones Constitucionales*, vol. 5, no. 1, 2018, 296-297.
[2] K. Schwab, *La Cuarta Revolución Industrial*, Barcelona, Debate, 2016, 20-21.

percentage of the world's population has unconsciously given up a significant part of their freedom and privacy.

On the other hand, the advantage of global communication and access to almost-instantaneous information, as well as the existence of artificial-intelligence systems that feed on this information, has limited the capacity of nation-states to exercise democratic control. In this context, the need of political institutions that can establish an effective regulatory framework globally is imminent.[3] These institutions must be characterized by a preventive, rather than reactive, nature, thus, distancing themselves from rigid and inoperative national or supranational legal systems currently in existence.

It is precisely here, that the imminent need to study the legal implications of the development and use of artificial intelligence systems lies. The need to tackle this issue becomes an existential imperative in areas where fundamental rights of individuals may be seriously violated, such as health, taking into consideration that: "Successful modernization and rapid technological evolution have catapulted us into areas where we can and must act, without providing us with the vocabulary we need to adequately describe or name those areas and our options for action. (...) We tend to say that a new digital empire is being born. But none of the historical empires we know - neither the Greek, nor the Persian, nor the Roman Empire - was characterized by the features that mark the digital empire of today. The digital empire is based on features of modernity that we have not yet really thought about. It does not rely on military violence, nor does it seek to integrate politically and culturally distant areas into its own realm. It does, however, exercise an exhaustive and intensive, deep and far-reaching control that ultimately pushes any individual preferences and deficits into the open terrain: we are all becoming transparent". [4]

It is evident, then, that focus should be directed on these insights and on the sociological and legal analysis of both national and supranational liability regimes. The goal is to identify their shortcomings in relation to the challenges posed by the use of artificial intelligence and propose feasible and effective reforms. The ultimate objective is the establishment of a functional global regime for the assessment and recognition of legal liability and the fair allocation of risk across all the different sectors of society.

To contribute to this objective, the following analysis will focus on the liability regime of the Health Administration currently in force in Spain. It will consider not only current EU regulation but also the legislative projects that have not yet been enacted. The analysis will begin with the identification of the constitutional provisions and the legal norms that regulate this regime. Subsequently, it will assess the applicability of this regime to the damages caused using artificial intelligence in the provision of health services.

2. *The liability regime of the Health Administration in Spain*

The right to health protection is recognized in Article 43 of the Spanish Constitution, which imposes the duty on public authorities to organize and protect health, adopting preventive measures and guaranteeing the provision of the necessary services to individuals. Accordingly, Article 41 orders public authorities to maintain a public and universal Social Security system available for all citizens.

In application of these constitutional rights and guarantees, Law 14/1986, enacted on April 25th, 1986, created the National Health System (NHS) and configured healthcare as an improper public service, allowing the adoption of indirect-management formulas and making room for private initiative.[5] These legal provisions have made the Spanish healthcare administration extremely complex and heterogeneous, as it is made up not only of public institutions, which include regional services, but also of other types of institutions created on the basis of public-private models. Health-care service providers, including public authorities, can thus avail themselves of a wide array of legal forms, including the concession of the management of the services to private entities.

[3] U. Beck, *El riesgo de la libertad digital. Un reconocimiento demasiado frágil*, in *Cuadernos del Mediterráneo*, no. 22, 2015, 313-314.
[4] *Ibidem*, 313.

[5] M. Cueto Pérez, *Responsabilidad Patrimonial de la Administración y Gestión Privada de Servicios Sanitarios - Incidencia de las Leyes 39/2015 y 40/2015 en el Modelo Actual*, in *Derecho y Salud*, vol. 26, 2016, 334.

The heterogeneous nature of the entities and organizations that provide healthcare services in Spain has caused problems regarding the definition of the liability regime applicable to their actions or omissions. However, the enactment of the twelfth additional provision of the now repealed Law 30/1992, which stated the Legal Regime of the Public Administrations and Common Administrative Procedure (LRJPAC), allowed a peaceful application of the liability regime provided on article 106.2 of the Spanish Constitution and in article 139.1 of Law 40/2015.

The liability regime for institutions that are part of the NHS is currently opaque, particularly considering the suppression of the Additional Provision enacted by Laws 39/2015 and 40/2015. This is further complicated by case law that subjects private-law entities that provide health services, to the private–instead of public–liability regime provided in Articles 1902 and 1903 of the Civil Code.[6]

However, since this paper focuses on the liability for the use of artificial intelligence by the Public Health Administration in Spain, undoubtedly the applicable legal regime is the one provided in Article 32.1 and 32.2 of Law 40/2015, that regulates the Legal Regime of the Public Sector (LRJSP): "1. Individuals shall have the right to be compensated by the corresponding Public Administrations for any injury they suffer to any of their property and rights, when the injury is a consequence of the normal or abnormal operation of public services, except in cases of force majeure or damages where the individuals, or private entities, have the legal duty to bear in accordance with the Law. (…) 2. In any case, the alleged damage must be effective, economically assessable and individualized in relation to a person or group of persons".

This general provision has not been further regulated for specific cases or purposes. Spanish legislation lacks specialized regulations and infra-legal dispositions to adapt the regime to specific activities or sectors of the Public Administrations. This lack of regulation has given an enormous discretion to judicial bodies in the application of this regime, particularly, when defining its main characteristics. In this regard, case law lack homogeneity. Contradictory rulings are widespread, especially regarding legal requirements for liability, such as the need for fault in the conduct of the Public Administrations and the legal duty of the private parties to bear the damage in accordance with the Law.

Nonetheless, the majority of the Spanish jurisprudence agrees that the liability of the Public Administration recognized in the aforementioned article is: a) unitary, as it applies to all the Public Administrations provided for in Article 149.1.18 of the Spanish Constitution; b) general, as it refers to all the activities and inactivities of the Administration, whether legal or factual; c) direct, as it falls on the Administration and not on the public official acting on its behalf, and, finally; d) strict or objective, as fault is not supposed to be a relevant factor in determining liability. Nevertheless, courts normally require some degree of fault in the underlying administrative action upon which the claim is based, to recognize the right of individuals, or private entities, to be compensated.[7]

As mentioned before, since the inception of this liability regime in the 1950s, its application has presented enormous challenges to judicial entities. These challenges will undoubtedly increase with the implementation of new technologies for the provision of public-health services. This is due to the fact that the use of systems or machines with artificial intelligence in the provision of health and/or paramedical services casts doubt on the usefulness of the classic requirements that are essential for the recognition of liability against Public Administrations.

These requirements will be analyzed from the perspective of the possible damages that the use of artificial intelligence may cause to individuals. In addition to this, we will identify certain legislative reforms that should be implemented to adapt to the new landscape derived from the invention of new autonomous and artificially-intelligent tools.

[6] M. Cueto Pérez, *Responsabilidad Patrimonial de la Administración y Gestión Privada de Servicios Sanitarios*, 360-361.

[7] L. Martín Rebollo, *La Responsabilidad Patrimonial de las Administraciones Públicas*, in *Manual de las Leyes Administrativas*, 3th Ed, Cizur Menor, Aranzadi Thomson Reuters, 2019, 11.

3. *The liability of the Spanish public health administration for damages caused using artificial intelligence*

The judicial application and interpretation of Article 32, which regulates the right recognized in article 106.2 of the Spanish Constitution,[8] has identified three main requirements for the Public Administration to be held liable for the actions or omissions of its officials. The first, consists of the existence of a compensable injury, understood as actual, real, economically assessable, individualized damage to a person or a group of persons, and unlawful, i.e., that the affected party does not have the legal duty to bear. The second, comprises the existence of an action or omission of the Health Administration, in charge of the operation of public services. And finally, the third requirement involves a direct and immediate causal relationship between the action or omission and the injury suffered by the individual.[9]

In this sense, the claimant seeking compensation from the Public Administration for injuries caused by its services must, in principle, prove each of the elements set out above. Under the general-liability regime this burden of proof already represents a real obstacle for victims. In regards to liability caused by the use of artificial intelligence, this burden will increase significantly, since this type of technology is characterized by: the opacity of its decision-making processes,[10] its technical complexity, its enormous openness to new information and its frequent necessity of information inputs once they have been put into circulation.[11]

This first challenge highlights the need for reforms to the regime of Public Administration's liability, by means of specific regulations, aimed at the prevention of this type of obstacles. This is especially necessary in the healthcare field. Undoubtedly, this difficulty should not cause the Health Administration to be irresponsible when it uses artificial-intelligence systems in the provision of its services, so the legislator can opt for some alternatives that have already been identified by specialists, such as the inversion of the burden of proof for certain elements or the presumption of causality in disproportionate damages.[12]

The risks associated with legislative inaction are significant. The maintenance of the current deficient regulatory framework could have dire consequences, such as skepticism between patients who could benefit from treatments or surgeries where artificial-intelligence tools or machines are used. Thus, an inadequate legal framework may result in depriving NHS patients of the countless benefits that these technological advances offer.

3.1 *Existence of a compensable injury using artificial intelligence*

3.1.1. *Damages that can be caused using artificial intelligence*

Today's artificial-intelligence systems, by feeding on a large amount of data, can contribute to aspects such as the design of public-health policies, the diagnosis and treatment of diseases and the monitoring of the spread of contagious diseases.

However, the risks involved in the use of this type of technology in public institutions, hospitals and other entities that make up the NHS are also evident. For example, the information used by this type of system will generally consist of personal data, medical records and intimate or confidential patient information. Therefore, its creators or programmers must not only be subject to strict ethical principles, but also comply with legal requirements that guarantee the rights of individuals[13] and the protection of that information.

Despite the adoption of these measures, the malfunction or illegal use of systems with artificial intelligence can undoubtedly generate compensable injuries to individuals. The legal duty to bear such injuries could not be imposed, since these would unlawfully violate express provisions of the Organic Law

[8] Spanish Supreme Court Ruling of 22 December 1997.
[9] J. A. Hurtado Martínez, *Responsabilidad Objetiva Patrimonial de la Administración Sanitaria: Doctrina Legal del Consejo de Estado y del Tribunal Supremo*, in *Boletín de la Facultad de Derecho de la UNED*, no. 18, 2001, 304.
[10] D. Parra Sepúlveda and R. Concha Machuca, *Inteligencia artificial y derecho. Problemas, retos y oportunidades*, in *Universitas*, vol. 70, 2021, 6.
[11] European Commission, *Report of the Expert Group on Liability and New Technologies*, 2019, 33.
[12] *Ibidem*, 48.
[13] A. Platero Alcón, *Breves Notas sobre el régimen de responsabilidad civil derivado de los sistemas de inteligencia artificial: especial referencia al algoritmo de recomendaciones de Netflix*, in *Ius Et Scientia*, vol. 21, no. 1, 2021, 136.

3/2018 on Personal Data Protection and Guarantee of Digital Rights as well as other legal rules that prevent the disclosure of this type of information.

It has also been shown that the use of artificial-intelligence tools can, on certain occasions, give results or diagnoses biased by human prejudices, like race and gender.[14] In the health field, biased results can cause extremely serious injuries to individuals and even violations of human rights and fundamental principles such as equality and non-discrimination of especially-vulnerable sectors of the population.

Finally, there are also more obvious risks associated to the use of systems or machines with artificial intelligence by the Health Administration. These risks consist of injuries to protected legal assets such as health, physical integrity and even the life of individuals. In this regard, it is worth taking into account the possibility that artificial-intelligence systems may misdiagnose patients or, less frequently, where the malfunctioning of autonomous or semi-autonomous surgical robots, such as CyberKnife and AESOP, may have enormous repercussions on the health of patients.[15]

Therefore, it is necessary to properly update these legal systems to new technologies with the purpose of avoiding the proliferation of claims and lawsuits by patients. Taking also into account that the greatest challenges will continue to arise, especially when determining whether the damage can be considered unlawful or, on the contrary, whether the individual has the legal duty to bear it. This characteristic, which turns the damage into a compensable injury, has brought enormous difficulties to Spanish jurisprudence, to the point of demanding fault of the administrative action or omission despite the applicable legal regime is supposedly objective or strict.[16]

In the healthcare field, the case law of the Supreme Court has seen the need to exclude from the supposedly strict-liability regime, the so-called medical acts themselves, where the application of liability criteria based on negligence for breach of the *lex artis* is inherent.[17] In this sense, since the nineties, the specialized doctrine has pointed out: "Within this progressively profiled panorama that the matter presents today, one can detect, on the one hand, as in so many other areas, a tendency towards the objectification (becoming strict) of liability. An objectification that seeks to offer reparation to the victims of the damages that are frequently inflicted on users in these complex care establishments that attend to them, responding to criteria of social solidarity rather than of strict culpability. However, alongside this perceptible tendency, the idea that the personal liability of the physician or any other healthcare professional can only be based on guilt, that is, on the personal reproach ability of his or her conduct, remains firm. This idea is firmly anchored in the case law of the Supreme Court and means, in the end, that the aforementioned objective (strict) nature of health liability extends to the public health service authorities, or even to private healthcare centers, but not to the medical professional as such".[18]

This differentiation between public health services and medical acts must be considered when analyzing the liability of the Health Administration for the use of systems with artificial intelligence, especially because this type of technology can cause damage in both areas of public service. On one hand, programs (*software*) with artificial intelligence used to facilitate the provision of public-health services are obviously capable of causing damage to their users. On the other hand, it is also possible that medical acts, performed by surgical robots, cause damage to patients.

In addition, the Health Administration can also be held liable for damages caused by defective artificial-intelligence systems, since

[14] G. Laín Moyano, *Responsabilidad en inteligencia artificial: Señoría, mi cliente robot se declara inocente*, in *Ars Iuris Salamanticensis*, vol. 9, 2021, 199.

[15] T.G. García Micó, *Litigación asociada a la cirugía robótica en el Da Vinci*, in *InDret – Revista para el análisis del Derecho*, no. 4, 2014, 10-11.

[16] O. Mir Puipelat, *Responsabilidad objetiva vs funcionamiento anormal en la responsabilidad patrimonial de la Administración sanitaria (y no sanitaria)*, in *Revista Española de Derecho Administrativo*, no. 140, 2008, 646.

[17] Spanish Supreme Court Ruling No. 1806/2020 of 21 December 2020; Spanish Supreme Court Ruling No. 50/2021 of 21 January 2021; Spanish Supreme Court Ruling No. 92/2021 of 28 January 2021; Spanish Supreme Court Ruling No. 824/2021 of 9 June 2021; Spanish Supreme Court Ruling No. 1340/2021 of 17 November 2021; Spanish Supreme Court Ruling No. 1423/2021 of 1 December 2021; and Spanish Supreme Court Ruling No. 272/2022 of 3 March 2022.

[18] J. Pemán Gavín, *La responsabilidad patrimonial de la Administración en el ámbito sanitario público*, in *Documentación Administrativa*, no. 237-238, 1994, 285.

their acquisition is related to the organizational part of the health services and not to medical acts themselves.[19] In these cases, strict liability should be applied more rigorously.

3.1.2. *Criteria for determining the unlawfulness of damages caused using artificial intelligence*

In order to avoid the existence of contradiction in judicial decisions regarding the unlawfulness of the damage, criteria have been developed, first in jurisprudence and later in law, to determine whether or not the individual has the legal duty to bear the damage.

As mentioned above, one of these criteria constantly applied by Spanish jurisprudence, especially in the healthcare field, is that prescribed in Article 34.1 LRJSP: "Article 34. Indemnification. Compensation shall only be payable for injury to the individual arising from damage which he has no legal duty to bear in accordance with the law. Damage arising from facts or circumstances which could not have been foreseen or avoided according to the state of knowledge of science or technology existing at the time of their occurrence shall not be compensable, without prejudice to the assistance or economic benefits which the laws may establish for these cases".

The application of this criterion, commonly known as *lex artis*, was of vital importance in resolving cases regarding the liability of the Health Administration for contagion with the HIV or Hepatitis C virus to patients who underwent blood transfusions. In AIDS-related cases, the Supreme Court determined that until 1985, the state of the art did not enable the detection of the HIV virus in blood. Therefore, all transfusions performed prior to that year did not give rise to liability on the part of the Health Administration because the injury was not unlawful.[20] In other words, when the state of scientific knowledge prevents the Health Administration from knowing the potential risk of causing the damage, individuals have the legal duty to bear it.

The proven usefulness of this guiding criterion, which is closely related to the due diligence of doctors or nurses when providing healthcare services, led to its inclusion in the cited legal disposition. However, its application by the case law of the Supreme Court has not been limited to medical acts *per se*, but has also been extended to the provision of healthcare services in general, which undoubtedly seems excessive and contradictory to other rulings of the same judicial entity.[21]

The vagueness in the application of this criterion by judicial institutions means that its application to damages produced by AI machines or programs may be detrimental to the users of the healthcare system, considering that the knowledge of the risks and consequences of AI is still extremely limited.[22] This type of technology is still unpredictable, especially because it can learn autonomously by constantly feeding itself with new information and because the risks to humans are still unknown to the science. Therefore, as the autonomy of robots and AI machines increases, the irresponsibility of the Health Administration in these cases will clearly become the general rule in application of article 34.

On the other hand, unlike the criterion analyzed above, the existence of prior and informed consent on the part of the victim can be useful when determining the unlawfulness of the damage, especially in cases of Health-Administration liability for the use of AI. In such cases, the patient´s lack of knowledge of the risks should be considered at the time of undergoing an intervention or treatment. It is precisely this type of area of administrative activity that represents a greater risk for individuals, so it is essential that they are guaranteed the possibility of deciding for themselves within the scope of their individual sphere and autonomy of will.[23]

In this regard, Spanish jurisprudence has

[19] M. Cuerto Pérez, *Jurisprudencia en el caso Ala Octa: Responsabilidad Patrimonial por la utilización de Productos Defectuosos en el Ámbito Sanitario*, in *Revista de Administración Pública*, no. 217, 2022, 178-183.
[20] M. Ortiz Fernández, *La Responsabilidad Civil Derivada de los Daños Causados por Sistemas Inteligentes y su Aseguramiento - Análisis del Tratamiento ofrecido por la Unión*, Madrid, Dykinson SL, 2022, 116.
[21] M. Cueto Pérez, *op. cit.,* 186-187.
[22] C. Gómez Liguerre and T. García-Micó, *Responsabilidad por uso de Inteligencia Artificial y otras tecnologías emergentes*, in *InDret - Revista para el Análisis del Derecho*, no. 1, 2020, 509.
[23] A. L. Rivas López, *Responsabilidad Patrimonial de la Administración Sanitaria (aspectos de su práctica administrativa y procesal)*, Málaga, Fundación Asesores Locales, 2012,117.

stated: "The specific content of the information transmitted to the patient to obtain his consent may condition the choice or rejection of a given therapy because of its risks (...) the prior information may also include the benefits to be derived by the patient from doing what is indicated and the risks to be expected otherwise (...)".[24]

Due to the above, in addition to what is prescribed in article 2.2. of Law 41/2002, which regulates Basic Patient Autonomy, the Health Administration should be legally required to inform patients or users of both the risks and benefits involved in the use of artificial intelligence, as well as the risks and benefits involved in not subjecting them to surgical interventions or treatments where this type of technology is used. Thus, in the event of a claim, the damage would not be considered unlawful if there was prior consent by the patient to subject him/herself to the risky use of AI. On the contrary, if the Health Administration cannot prove the existence of such consent, the judge should consider that the individual does not have the legal duty to bear the compensable injury.

In other words, the application of the *lex artis* can exonerate responsibility on the part of the Health Administration, in cases where there is little knowledge of the risks, as in the case of the use of AI, but it can be useful when one of its manifestations, such as the patient's prior and informed consent, is correctly applied.

However, additional legal or jurisprudential criteria should be identified[25] to provide objectivity and predictability to the liability regime of Public-Health Institutions, for the benefit of patients analyzing the feasibility of filing a claim. Considering, moreover, that the unlawfulness of the injury is an element commonly used by case law to reject the liability of the Public Administration,[26] precisely because of its abstract and vague nature.

3.2. *Action or omission of the Public Administration*

The liability of the Health Administration for the use of AI can arise from the material conduct of its public servants, whether they are doctors, nurses, assistants or even providers of paramedical services such as cleaning, maintenance and, obviously, IT. However, the use of AI is not limited to this type of activity of the Health Administration as it can also be employed in the technical motivation of formal acts, of regulatory and/or administrative nature.

Furthermore, it cannot be ruled out that, soon, autonomous AI systems will be used to issue formal acts for the Public Administration, and their annulment may be subject to liability. In this sense, their annulment may occur under various circumstances such as a technically erroneous motivation or fundamental-rights violation.

Nevertheless, as the administrative formal acts are indisputably attributable to the Public Administration, there are greater challenges in cases of the participation of the systems with IA in material actions. Considering that the IA can replace, totally or partially, the conducts of the public servants, it becomes necessary to analyze what the doctrine calls the first-level imputation in this type of cases.

3.2.1 *First-level imputation - attribution of the conduct to the Health-Care Administration*

According to doctrine, the application of the first-level imputation requirement entails an analysis of those instances in which a conduct, carried out by a natural person, can be attributed to the Public Administration. Therefore, it can be stated that there has been a functioning of public services.[27] In this sense, all the actions or omissions of natural persons, who are integrated in the administrative organization and who act in the exercise of their legal roles will be imputable to the Administration.[28]

Likewise, due to the fact that health

[24] Spanish Supreme Court Ruling of 4 April 2000 - RC 8065/1995.

[25] There are authors who recognize as a guiding criterion on the clinical situation of the patient, which is also applicable to cases of the use of artificial intelligence. Clearly, cases in which the patient is admitted with a critical situation cannot be treated as those in which the patient is admitted in a stable situation (J. E. Rebés Solé, *La Responsabilidad Patrimonial por asistencia sanitaria desde la perspectiva de los órganos consultivos*, in *Revista Española de la Función Consultiva,* no. 1, 2004, 90).

[26] J. Guerrero Zaplana, *Las peculiaridades de la Responsabilidad Patrimonial de la Administración Sanitaria: El criterio de la Lex*, in *La Responsabilidad Patrimonial de la Administración Sanitaria*, Madrid, Consejo General del Poder Judicial, 2002, 82 - 83.

[27] O. Mir Puigpelat, *La Responsabilidad Patrimonial de la Administración Sanitaria - Organización, Imputación y Causalidad, Madrid*, Civitas Ediciones, 2000, 43.

[28] O. Mir Puigpelat, *op cit.,* 144.

activity is legally configured as a public service, the Health Administration is also liable for: a) injuries caused by the conduct of natural persons belonging to private-law entities, which were created by the Health Administration for the provision of health care; and b) injuries caused by private contractors, in compliance with an order or obligation expressly imposed by the contracting entity itself.[29] All this is based on the provisions of article 121.2 of the Law of Forced Expropriation[30] and article 32.9 LRJSP.

However, the use of AI systems by the Public Administration in general, and by the Health Administration in particular, may result in the recognition of liability for those conducts carried out by subjects specifically identified for this technology.

In this sense, AI specialists initially considered that the liability for damages caused by AI systems or products lies on the manufacturer, the designer, the hardware developer, the operator, the owner or the user, depending on the subject that could have anticipated, foreseen and prevented its malfunction or illegal use. Albeit, currently, it seems more convenient to simplify these subjects into two categories: the first one called *Back End* operators includes the person who operates the system, but does not use it (updates the software, introduces improvements, reviews and monitors); and the second one called *Front End* operators, which are the individuals who operate the system and use it or benefit from it (examples: owner, user or holder).[31]

Although such subjects have been identified for the scope of civil liability, which is characterized by being based on fault, they can also be applied to the Public Administration's liability regime. Thus, demonstrating the importance of the recently enacted Artificial Intelligence Act,[32] since there was no special regulation either at European level, or in Spain.[33]

The enactment of this Act will surely nurture the Public-Administration liability regime with these types of concepts and facilitate the regulation of this legal regime, since it seems reasonable to consider that the conduct of individuals included in *Front End* and *Back End* categories can lead to the Health Administration being obliged to compensate individuals for damages caused using AI. This considering, firstly, that the Administration is included in the *Front End* category when it is the owner, user or possessor of this type of technology. In less frequent cases, it could also be included in the *Back End category*, when the subjects responsible for updating the software, introducing improvements, reviewing and supervising this type of systems, are contractors or public servants belonging to the Health Administration. This implies that the Health Administration should be liable for the conduct of *Back End* operators when the conditions prescribed in the legal provisions of the LEF and the LRJSP are met.

However, the actual lack of specific regulations on liability for the use of AI, forces the application of the consumer-defense legislation contained, at the European level, in Directive 85/374/EEC of July 25, 1985 and, in Spain, in the General Law for the Defense of Consumers and Users.[34] This focuses solely on the liability of the producer or manufacturer and, therefore, excludes from its scope of application the other agents involved in the operation of an AI product,[35] which will make it difficult to apply liability to the Health Administration.

In this regard, Spanish case law has pointed out that: "*the objective (strict) nature of the liability provided in the aforementioned legislation on consumers and users does not include, extend to or cover the so-called "medical acts themselves"* ", such as surgical interventions. Consequently, the Supreme Court has rejected the liability of the Health Administration when this is caused using defective products in surgical interventions, especially when such defects have been alerted after their application.[36]

[29] *Ibidem*, 128.
[30] In the provision of public services, the compensation shall be borne by the concessionaire, except in the event that the damage has its origin in some clause imposed by the Administration on the concessionaire and which is unavoidable for the latter to comply with.
[31] G. Laín Moyano, *op cit.,* 206.
[32] COM (2021) 206 - Brussels, 21 April 2021.
[33] On this regard review: M, Ortíz Fernández, *La Responsabilidad Civil Derivada de los Daños Causados por Sistemas Inteligentes y su Aseguramiento - Análisis del Tratamiento ofrecido por la Unión Europea*, Madrid, Dykinson SL, 2022, 72 -81.
[34] Real Decreto Legislativo No. 1/2007 of 16 November 2007. Boletín Oficial del Estado No. 287, of 30 November 2007.
[35] M. Ortiz Fernández, *op. cit.,* 64-68.
[36] Spanish Supreme Court Ruling No. 1806/2020 of 21

Based on these considerations, case law has been inclined to conclude that liability falls on the producer or manufacturer and on the public institution responsible for guaranteeing and controlling quality. Limiting the application of a strict liability regime to the Public Administrations obliged to control the use of artificial-intelligence systems and excluding its application to the Health Administrations that provide services using this type of technology.

On the other hand, it is highly unlikely that public institutions intervene as manufacturers or producers of AI systems to justify an application of this regime to institutions of the NHS. Likewise, the application of this regime to cases in which the manufacturer or producer is a public contractor is obviously complicated.[37] Especially, due to the challenge of qualifying certain AI systems as defective products, given that they are not in the nature of tangible goods.[38]

Therefore, it is vital to enact specific legislation regulating liability for the use of AI and to create an administrative institution to control its quality, otherwise it would be difficult for victims to hold the Public Administration responsible or co-responsible for injuries caused by this type of technology.

3.2.2. *Liability-imputation titles*

In accordance with the provisions of article 32 LRJSP, the basic criteria in the liability regime of the Health Administration lies in the administrative ownership of the activity or service in which the damage has occurred. Thus, when the victim proves that the injury was caused in the performance of an activity whose ownership corresponds to an Administration, the latter will be obliged to compensate.[39]

In other words, the healthcare administration can now be held responsible even for the conduct of its non-healthcare personnel (statutory),[40] which includes the computer technicians responsible for the proper functioning of the systems that use AI.

However, as technological development grants greater autonomy to this type of systems, their use by the Health Administration will bring additional difficulties regarding liability. Although there is still no such thing as strong AI, understood as an AI that can perform the same intellectual tasks as a human being,[41] its use in the future cannot be imputed to the Health Administration, since the current regime is designed to be applied to human conducts.

On this point, it is important to analyze the advisability of future legislative reforms so that autonomous robots using strong artificial intelligence are recognized as electronic persons, and therefore, the possibility of holding the Health Administration liable for the actions or omissions of electronic public servants. In this regard, I find convincing the experts' position that the legal recognition of electronic persons generates more problems than solutions, mainly because it exempts their manufacturers, operators, or programmers from liability.[42]

For the time being, it seems sufficient that the provisions of article 121.2 LEF and 32.9 LRJSP are not limited to the concessionaire but apply also to contractors and other parties involved in the operation of an IA system or machine. Thus, it should be specified that the liability of the Health Administration needs to be recognized in cases where it is not clear whether the damage is attributable to the *Back End* operators of the IA system, or to their *Front End* operators (where the Health Administration is included). In the same sense, the liability should be expressly recognized in cases where the damage is caused by a contractual clause imposed by the Administration unavoidable for the contractor.

The above is related to another liability criterion foreseen by the European Artificial Intelligence Act, which could be adjusted to the Health-Administration liability regime. This liability criterion consists of the risk generated by the AI and determines that the person who can control this risk and benefits from its operation, should be the one held

December 2020; Spanish Supreme Court Ruling No. 50/2021 of 21 January 2021; Spanish Supreme Court Ruling No. 92/2021 of 28 January 2021; Spanish Supreme Court Ruling No. 824/2021 of 9 June 2021; Spanish Supreme Court Ruling No. 1340/2021 of 17 November 2021; Spanish Supreme Court Ruling No. 1423/2021 of 1 December 2021; and Spanish Supreme Court Ruling No. 272/2022 of 3 March 2022.

[37] G. Laín Moyano, *op. cit.,* 212.

[38] Consider article 136 of the Spanish General Law for the Defense of Consumers and Users.

[39] O. Mir Puigpelat, *op. cit.*, 54.

[40] *Ibidem*, 171 -172.

[41] G. Laín Moyano, *op. cit.,* 201.

[42] C. Gómez Liguerre and T. García-Micó, *op. cit.,* 506 - 509.

liable.[43] In other words, the liability falls on the *Front End* operator which, in this case, is the Health Administration, mainly because this is the only one that controls the conditions under which the health service is provided and, consequently, is able to control the risk to which patients are subject at the time of using such technology.

Using this criterion, the aforementioned Act gives a differentiated treatment to the following categories of sectors, uses or purposes of artificial intelligence: on the one hand, there are the high-risk ones and determined by inclusion in an exhaustive and cumulative list, and, on the other hand, the low-risk ones, determined by logical exclusion with respect to the previous ones.[44] The provision of public services entrusted to the Healthcare Administration unquestionably falls into the first category, together with, for example, self-driving cars and AI systems in financial and stock-market matters that allow users to decide where to invest in the stock market, etc. Such uses or sectors obviously generate greater risks than those that could be caused by a smart speaker.[45]

The interesting aspect about this differentiation with respect to the liability of the Public Administration is that the sectors that represent a high risk would be subject to a regime of strict liability, and, on the contrary, those of low risk would be subject to a regime of subjective liability or negligence-based liability.[46] Therefore, the liability regime of the Health Administration currently applied in Spain coincides with the liability regime that the European Union impose specifically on the use of AI in the health sector.

Even in the *Liability Report for Artificial Intelligence and other emerging digital technologies*, the group of high-level experts expressly point out that the recognition of strict liability is an appropriate response to the risk generated by the use of emerging digital technologies, especially when these technologies are being used by public entities and significant damage can be caused to individuals.[47]

The liability of the Health Administration for the use of AI should be based on the risk that this use entails for the patients of the Spanish National Health System.

However, regarding risk as a liability criterion, it is necessary to take into account the case law of the Supreme Court that has rejected the liability of the Health Administration for the use of defective products, considering that in these cases the risk does not derive from the application of the product or from the medical act, but from its manufacture and the lack of control by the Public Administration.[48] Such consideration, undoubtedly, will also be applied with the purpose of disregarding the liability of the Health Administration that uses AI in medical acts and in the provision of health services in general.

3.3. *Causal relationship between the conduct and the damage – second-level imputation*

This third element of the Health Administration's liability is called by some authors as second-level imputation, as it analyzes the relationship that must exist between the damage and the operation of the public service for the Administration to be obliged to pay compensation, as opposed to first-level imputation which, as detailed above, analyzes the relationship between the conduct and a specific subject responsible for its consequences.[49]

Spanish case law initially required a direct, immediate, and exclusive causal relationship to recognize the liability of the Health Administration. Subsequently, the Supreme Court has pointed out that it cannot exclude the possibility that this causal relationship may appear under other more mediate, indirect, or concurrent forms that may or may not cause a moderation in the liability.[50]

However, the recognition of the causal nexus in such a broad sense seems to cause

[43] *Ibidem*, 508.
[44] A. Tapia Hermida, *La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento*, in *Revista Ibero-Latinoamericana de Seguros*, vol. 30, no. 54, 2021, 118.
[45] A. Platero Alcón, *op. cit.,* 137.
[46] *Ibidem,* 139-141.
[47] European Commission, *Report of the Expert Group on Liability and New Technologies*, 2019.
[48] Spanish Supreme Court Ruling No. 1806/2020 of 21 December 2020; Spanish Supreme Court Ruling No. 50/2021 of 21 January 2021; Spanish Supreme Court Ruling No. 92/2021 of 28 January 2021; Spanish Supreme Court Ruling No. 824/2021 of 9 June 2021; Spanish Supreme Court Ruling No. 1340/2021 of 17 November 2021; Spanish Supreme Court Ruling No. 1423/2021 of 1 December 2021; and Spanish Supreme Court Ruling No. 272/2022 of 3 March 2022.
[49] O. Mir Puigpelat, *op. cit.,* 44.
[50] A. L. Rivas López, *op. cit.,* 109.

that, in certain circumstances, it is confused with the unlawfulness of the injury. As, for example, in cases where it is considered that the negligent and deliberate conduct of the injured party himself breaks the causality relation, when in fact such action or omission imposes the legal duty to bear the damage, since it is the patient who placed himself/herself in the situation of risk.[51]

Based on the above, especially in cases of use of AI by the Health Administration, it seems appropriate to apply the theory of objective imputation, which rejects legal considerations when determining the causal link and argues that causation will always be a naturalistic, empirical notion, completely independent to normative-valuative considerations.[52] Therefore, the causal relationship between the use of AI by the Health Administration and the compensable injury caused to the individual should always be determined based on technical or scientific considerations.[53]

It is mainly the regulation of these criteria for assessing the causal relationship that the European Union seeks with the issuance of the Proposal for a Directive of the European Parliament and of the Council on adapting non-contractual civil liability rules to artificial intelligence (AI Liability Directive),[54] by stating in the explanatory memorandum that: "In the public's view, the "black box" effect may make it difficult for the victim to prove fault and causation, and may create uncertainty as to how the courts will interpret and apply existing national liability rules in cases involving AI".

Based on these considerations, the Proposal for a Directive regulates non-contractual civil liability, without ruling out that its provisions may be applied to the Public-Administration liability regime. It also provides provisions aimed at easing the burden of proof in a very specific and proportionate manner, through the use of the production of relevant evidence relating to specific high-risk AI systems suspected of having caused damage (Article 3); and rebuttable presumptions (*iuris tantum*) regarding the causal link between the defendant's fault and the results produced by the AI system or the non-production of results by the AI system, when certain special conditions are met (Article 4).

Finally, in the field of artificial intelligence, there are complications in the circumstances where causality is broken, such as force majeure or other cases where the jurisprudence applies a concept known as concurrence of causes.

Regarding force majeure, case law has indicated that the rupture of the causal link is given by an event that has been irresistible, even in the case that this could be foreseeable and external, in the sense that this is alien to the service and the risk that is proper to it.[55] Based on these characteristics, a clear example in the field of AI would be the malfunction of a surgical robot during surgery, due to a sudden power failure caused by a traffic accident. Evidently, in this case the damage was caused by causes beyond the control of the Health Administration that have no relation to the risk that the use of AI represents to the patients of the NHS.

The legal concept of force majeure cannot be associated with *lex artis*, since the latter is not related to the rupture of the causal nexus, but to the legal duty that the legal system imposes on the individual to bear the damage caused by the Health Administration. This differentiation is evident in the development of Spanish case law with respect to HIV infections, which were initially considered as cases of force majeure because they were irresistible according to the state of knowledge at the time the damage was caused, and, since the rulings of the Supreme Court of 1 and 6 November 2001, have been considered as cases in which the unlawfulness of the damage is absent, since they are not external and independent of the risk caused by the health service.[56]

Such considerations are important in damages caused by the use of AI, since such technology, as mentioned above, causes difficulties in determining whether the causes are external to the risk and the health service, being caused by errors made by manufacturers or programmers, or internal, being properly related to the Health Administration. Considering that, in the second case, if such causes are also undetermined or unknown, we would be facing a fortuitous event, for which the Health Administration would also be

[51] *Ibidem*, 111.
[52] O. Mir Puigpelat, *op. cit.,* 69.
[53] *Ibidem,* 225 - 250.
[54] COM (2022) 496 - Brussels, 28 September 2022.
[55] Spanish Supreme Court Ruling of 31 May 1999.
[56] A. L. Rivas López, *op. cit.,* 116.

responsible.[57]

On the other hand, there are cases where the compensable damage is not caused by a single cause, but by several technically relevant causes. In these cases, case law applies the concurrence of causes and modulates the liability of the Public Administration, ordering it to pay the proportional part of the compensation.

The aforementioned figure can be useful in the field of IA, where the Health Administration proves that the damage was not exclusively caused by the provision of the public service, but that the relevant conduct of other operators, such as the programmer or manufacturer, also had an influence. In this sense, it should be the Health Administration that is obliged to demonstrate the confluence of different causes since, in cases where there is doubt as to whether it is the conduct of the Health Administration or of another operator that caused the damage, it would be advisable that the former should be liable for compensation.

4. *The application of a strict liability regime to the use of artificial intelligence by the Health Administration*

Article 32 LRJSP, by maintaining the sense of the previous legal provisions and prescribing that individuals have the right to be compensated for any injury resulting from the normal or abnormal operation of public services, evidently recognizes an absolute strict-liability regime that theoretically should not admit exceptions.[58] However, case law has found it necessary to impose limits such as the application of the state of knowledge or *lex artis*, which clearly prevent fault from being totally irrelevant in the analysis of the liability of the Health Administration and of the Public Administration in general.

In this way, it is evident that the elements of fault are introduced into the analysis, by the jurisprudence, using the requirement of the unlawfulness of the damage. This ambiguous requirement has caused enormous legal uncertainty to individuals and has been commonly applied to reject obvious liability of Public Administrations.

The problems that the unlawfulness of the injury has generated at the time of applying the regime of liability of the Administration are not new but have existed since enactment of the regime in 1954. However, with the emergence of these new technologies, which can be used by the Administration to provide public services, the difficulties will surely increase if minimum predictability is not granted to the regime.

In this sense, the legal system should not only require that the legal duty of the individual to bear the damage is expressly prescribed in the Law, as is the case of *lex artis* and informed consent, but also that some of these criteria be specifically regulated for cases of liability for the use of artificial intelligence. Additional procedures and parameters should be established to adapt the criterion of the unlawfulness of the injury to the reality of new technologies.

On the other hand, the recognition of a global regime of liability, applicable to all administrative activity, cannot be the best option. Instead, what is clearly advisable is the recognition of a differentiated regime of subjective liability for certain areas of administrative activity and of strict liability for others. As established in the Artificial Intelligence Act, which determined a strict liability regime for the use of AI that generates high risk to users and a subjective regime for the use that generates low risk.

In the field of the use of AI by the Health Administration, the criterion of the specialists seems to coincide with the strict-liability regime currently in force in Spain. Firstly, because this type of liability was rightly developed, during the 19th century, as a response to the risks brought about by the new technological developments of the industrial revolution, which makes it ideal for the challenges posed by the use of AI, and, secondly, because it is difficult to determine the perpetrator of the negligent conduct when using this type of technology. So, it is convenient that this determination becomes irrelevant.[59]

In this sense, the Report of the Group of Experts, while stressing the importance of the coexistence of liability regimes within each EU member, highlights an additional advantage of the application of a strict-liability regime to the use of emerging technologies. This type of liability spares the

[57] *Ibidem*, 113.
[58] O. Mir Puigpelat, *op. cit.,* 69.
[59] European Commission, *Report of the Expert Group on Liability and New Technologies*, 2019, 25.

victim the impossible task of identifying the breached standard of care, taking into consideration that standards of care were designed for human conduct.[60]

On the other hand, as a disadvantage of the application of strict liability to the use of emerging technologies, specialists point out the impact that this recognition can have on their use and development. This consideration applied to the field of public healthcare may dissuade healthcare administrations from acquiring this type of tools, due to the risk represented using artificial intelligence and the high probability of being held liable for its use.

However, the consequences of applying a negligence-liability regime to the use of AI by the Health Administration may be greater, since in this case the individual would be discouraged from undergoing treatments or therapies that use artificial intelligence.

Therefore, a convenient solution is the one proposed by the theory of increased liability of the owner of a robot. This theory developed from the idea of the difficulty of proving the negligence of the owner, the defect of the product or the causal link, to subsequently conclude that the owner should be strictly liable for the damages caused to third parties, but with the recognition of a limit to such liability.

Applying this limit of liability to the Health Administration, which will generally own the robot or AI system, may avoid the deterrent effects mentioned above.

5. *Conclusions*

The use of systems or devices involving artificial intelligence by the Health Administration presents important additional challenges to the application of each of the requirements demanded by the liability regime provided in the Spanish legal system.

One of the main challenges is related to the diversity of the damages that these systems can generate and the application of the criterion provided in the first paragraph of article 34 of the Public Sector Legal Regime Law, related to the state of knowledge or *Lex Artis,* as a criterion to determine the unlawfulness of such damages. In this sense, in the field of the use of AI, the application of this criterion should be limited to protect the rights and interests of individuals and to avoid contradictory judgments.

On the other hand, there are enormous challenges regarding the victim's burden of proof, which is extremely complicated in cases where the compensable injury is caused by the use of AI, as this technology is highly opaque, complex, open to new information and vulnerable to cyber-attacks. This is one of the areas where legislative reforms, such as those contained in the Proposal for a Directive on the adaptation of non-contractual civil liability rules to AI, are going to be extremely necessary. Considering also that the enactment of this proposal would oblige Member States to establish specific regulations in this area and to update or adjust their liability regimes to these types of technologies.

Likewise, it is essential to adopt reforms in the imputation of liability, such as the recognition of rebuttable presumptions regarding causality and negligence in the defendant's conduct. In addition to this, with the development of autonomous robots with strong artificial intelligence, it will become even more difficult to impute their actions to the Health Administration which currently only acts through its public servants.

Finally, as the use of artificial intelligence in the healthcare field is of high risk, the legislative initiatives of the European Union recommend the application of a strict-liability regime, like the one currently recognized in Spain. However, this liability regime is extremely deficient in providing criteria that guarantee objectivity and predictability in its application. These deficiencies will be aggravated when applied to cases where the use of artificial intelligence by the Public Administration causes damages to individuals, as the risks associated with the use of this type of technology are indeterminate and extremely difficult to assess.

The implementation of a strict-liability regime for this type of cases, from the point of view of supporting innovation, should be limited. This limitation aims to prevent the Health Administration from being discouraged in acquiring this type of technology for the provision of health services, which would unjustifiably deprive patients of the enormous advantages that its use represents.

[60] C. Gómez Liguerre and T. García-Micó, *op. cit.,* 505-506.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 71-85
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 07

*HealthTech and AI in Hungary**

Miklós Zorkóczy
(Master of Medical Law (LLM), Partner at Zorkóczy Law Office, Lecturer at Peter Pazmany Catholic University, Faculty of Law)

ABSTRACT Consumers are keen on the use of technology. People trust in technology more and more. What is happening in the Health Sector? What solutions can be used and for what purposes? What is happening in the care service and on the patient's side? The study will evaluate the cooperation of healthcare and technology (HealthTech) from legal and technology point of view in the Hungarian Healthcare. The cooperation among legal and tech people is key when a medical malpractice occurr
Firstly, the law appoints the rules applicable in a certain case. Secondly, the product lifecycle of a medical device would tell who was liable for the malpractice. Besides introducing studies in medical sociology referring to the changes of the social impacts like the doctor – patient relationship in the online domain, this paper describes the laws to be used to find the liability clauses and demonstrates technology matters in the Hungarian jurisdiction.

1. *Introduction*

The lockdown during COVID19 amplified the online presence. Like people work online rather than in the office (home office). Instead of the weekly shopping, they order food from online platforms, also select technical goods in digital stores, *and even they buy clothes and shoes online. Consumers use technology and people trust in technology more and more. What is happening in the Health Sector? What technology can be used for what purposes? What is happening in the Health Society in the care service and on the patient's side? The study will evaluate the cooperation of healthcare and technology ('HealthTech') from legal and technology point of view in healthcare. The cooperation among legal and tech people is always key when a medical malpractice occurred. Firstly, the law appoints the rules applicable in a certain case. Secondly, the evaluation of the product lifecycle of a medical device would tell who was liable for the malpractice. Results of studies in medical sociology referring to the changes of the social impacts will show changes of the doctor – patient relationship. Besides these results, this paper describes the laws to be used to find the liability clauses and demonstrates technology matters in the mirror of the Hungarian Healthcare System.

2. *Emergency Legislation*

The patient – doctor touch facilitated the spread of the COVID. Besides the threatened people with chronic diseases, the medical staff was also in risk. On the other hand, patients still needed the diagnosis, therapy, advice, and prescriptions. The Government Decree on Telemedicine Applications[1] introduced a widespread engagement of this technology, and which regulation was later integrated into the higher legal hierarchy.[2]

When the "Health Emergency Situation" passed by, the Act on Healthcare[3] secured permanently the general rules of providing healthcare services by telemedicine applications. Further detailed rules were laid down by a Ministry Decree on Basic Requirements of Healthcare Service Providers.[4] Pursuant to Section 3 of the aforementioned Decree, the healthcare service must provide proper info - communication equipment, medical devices, telemedicine care procedures and notice to the patient with the information necessary for the health service provided by telemedicine. According to Subsection 1 of Section 9 of the Decree, it is the competence of medical staff to decide whether the characteristics of care and the medical professional judgement allow the performance of activities based on personal meetings through info-communication tools. In this way the doctor can make a diagnosis, provide therapeutic recommendations, counselling, arrange consultations, patient management, give referrals, prescribe medications.

*Article submitted to double-blind peer review.

[1] Government Decree no. 157/2020 (IV. 29.) and Decree of Health Ministry no. 33/2020 (IX. 16.) 'EMMI'.
[2] Act on Health Emergency (2020. évi LVIII.), Art. 85, § Section 2.
[3] Act on Healthcare (1997. évi CLIV.), Sections 106/A, 247.
[4] Decree of Health Ministry no. 60/2003 (X. 20.) 'ESzCsM', Section 3, Subsection 1, Point g.

Doctors are obliged to document the events of care realized in the form of telemedicine in of medical records. They need to keep records in the medical (praxis) software, in addition to symptomatology, the diagnosis, patient journey, time of control, referral, values measured at the patient's home, and in order to make contact bilateral, current contact details and current location must be kept.[5] Services provided via telemedicine tools are accepted by the National Health Insurance Fund as a type of care.[6]

Some groups of patients suffer from inequality like people who don't have internet access or the knowledge how to use it. They can easily be excluded from a digital service, especially people with disabilities. One study found that COVID19 has amplified digital inequalities because they are less able to adapt technology.[7] According to another research, digital health offers new opportunities for screening, prevention, and monitoring of homeless people.[8] In family and child protection issues the telecommunication tools are also usable.[9] Family and Child Protection Officers providing mediation services for conflict management are allowed to inquire about health status of the person concerned by phone contacting.[10]

Patients confirmed the popularity of telemedicine when 71% of the population requested a prescription online or by phone, so the use of technology transforms the doctor – patient relationship, the health management.[11] Based on the same survey, patients believe that technology makes healthcare more convenient, saves time, improves communication, and helps them get care faster though they think the malfunction of technology could jeopardize their healing.

Patients accepted the new technology in general, there are still some concerns for certain groups of people living with disabilities or in poor living standards.

3. *The Concept of AI in Healthcare*

In healthcare, artificial intelligence ('AI') refers to machine learning systems that help the physicians and the medical staff. Such systems could be Big Data analysis tools, image recognition and evaluation systems, language technology solutions. Healthcare professionals in Hungary use such tools in imaging diagnostics,[12] personalized precision medicine,[13] or drug developments that accelerate virtual clinical research.[14]

They can do it as AI is a kind of software that mimic human capabilities. In terms of technology, it is not just a software. It is a trained and tested machine working on a specific database. There are different types of AI technology based on models, applications, industries, functionalities. In the context of healthcare, let us now narrow down the scope to machine learning methods that support the healthcare system.

The Hungarian Law refers to the Medical Devices Regulation[15] (MDR) which defines the term as follows: 'a medical device is any instrument, appliance, apparatus, software, ... other article intended by the manufacturer for use in humans, alone or in combination, for one or more specific medical purposes.' An AI powered solution is embedded into a software code, and it has an interface to run the engine, and a database to learn from and to process.

The medical purpose could be diagnosis, prevention, monitoring, prognosis, treatment, mitigation of disease, or the diagnosis of injury or disability. Additional such medical purposes include the testing, replacement, or

[5] Zs. Győrffy (ed.), *Telemedicine During COVID-19 in International and Hungarian experiences and guidelines,* in *Medical Journal (Orvosi Hetilap)*, 2020, vol. 24, no. 161, 983-999.

[6] Decree on Health Ministry no. 9/2012 (II. 28.) 'NEFMI'.

[7] J. Boros, E. Girasek, B. Döbrössy and Zs. Győrffy, *Use of digital healthcare among people living with disabilities*, in *Hungarian Journal of Disability Studies & Special Education*, no. 2/2022, 77-78.

[8] Zs. Győrffy, S. Békási, B. Döbrössy, V. K. Bognár, N. Radó, E. Morva, Sz. Zsigri, P. Tari and E. Girasek *Exploratory attitude survey of homeless persons regarding telecare services in shelters providing mid- and long-term accommodation: The importance of trust*, Sungwoo Lim, New York City Department of Health and Mental Hygiene, United States, 2021.

[9] Decree on Health Ministry no. 35/2020 (X.5.) 'EMMI'.

[10] E. Gyulai, *The mediation in person and online in case of family contacts during pandemic,* in *Family Law*, no. 1/2021.

[11] E. Girasek, J. Boros, B. Döbrössy, A. Susánszky and Zs. Győrffy, *E-patients in Hungary: Digital skills in healthcare, traditions in the mirror of a national survey,* Semmelweis University, Medical Sciences, Behaviour Department, Budapest, 2022.

[12] www.kheironmed.com/mammography.

[13] https://oncompass.hu.

[14] https://turbine.ai.

[15] Article 2(1) of Medical Devices Regulation (MDR) no. 2017/745 of the European Parliament and of the Council.

modification of an anatomical, physiological and/or pathological process or condition. The provision of information by testing samples (organs, tissues and blood) from the human body - in vitro (i.e. outside the body, e.g. in a test tube or cup) is also included. The definition of a medical device accessory also complements the concept, as although not serving a medical purpose, when used in conjunction with a medical device, the accessory enables or facilitates the use of the medical device. An active device is one that satisfies its power requirement from outside the human body, such as software.

Previously, the Act on Healthcare[16] provided essentially the same, although slightly narrower definition of medical devices, which was incorporated into the text of the legislation with identical content. At the regulatory level, additional definitions can also be found depending on what the device is made of, how or for what purpose it is used, what purpose it serves.

Within the medical device category, a distinction should be made between medical devices and medical assistive devices,[17] which are medical devices or technical nursing equipment for the personal use of the patient, but which do not require the constant presence of a qualified medical professional and are typically used for diagnostic, therapeutic, rehabilitation or nursing purposes. All the devices must be listed in public registers.[18]

Legislation clearly defines the use of AI or any other technology used in medical devices, people and clinical staff can trust of the used systems since the technology must be validated and admitted by Government Authorities at the end of a successful clinical trial process. Changes in the EU Legislation like the proposed AI Act[19] will require further risk assessments of medical systems.

4. *Clinical Trial of Medical Devices*

There is a huge risk that people's health might be adversely affected by an inadequately tested and controlled product. The legislator has therefore developed a detailed set of procedures that guide applicant manufacturers through a series of stages. According to MDR,[20] a clinical trial is a documented series of events that produces a meaningful and measurable clinical outcome through the evaluation of evidence, under the personal responsibility of the investigator. The trial subject (i.e. participating patient) gives his/her prior informed consent in writing to any information that is relevant to his/her decision. The information should be given to the person concerned (data subject). This confirms his/her consent that it was voluntary and freely expressed to participate in the trial.

A clinical trial is initiated at the request of the manufacturer or developer by submitting the documentation to the competent Member State and entering it into the electronic system set up by the European Commission.[21] As regards the Member State level, in Hungary, the Medical Research Council (ETT) is an opinion and decision-making body of the Minister of Health. The Council is an independent body of experts that gives its opinion on the application. After having the opinion of the Council, the National Institute of Pharmacy and Food Safety[22] issues the official authorisation. If the specified procedural steps and deadlines are met, the device can be used on the basis of the authorisation to start a clinical trial. This requires the prior consent of the trial subject (patient). Whether or not a device is safe and fit for the intended purpose can be established after its clinical evaluation, which also ascertains that there is no more effective procedure, and that the risks to the trial subject are proportionate to the expected benefit and the research objective to be achieved.

The developer or manufacturer monitors the conduct of the research based on the approved trial plan and, if there is a change to the plan, it must be reported to the authority for re-authorisation. Adverse events and device failures occurring during the studies must be reported to the authority.

[16] Section 3 of Act on Healthcare.
[17] Act on the Safe and Economical Supply of Medicines and Medical Assistive Devices and on the Marketing of Medicines (2006. évi XCVIII.), Section 3, Subsection 6.
[18] PUPHAG – Public Medical Assisted Devices Register; SEJK – Online Device Database.
[19] Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, 2021/206 (COM).
[20] Article 2.44-59 of the MDR.
[21] Articles 61-82 of the MDR.
[22] Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet (OGYÉI). Please note, the authority was merged with National Health Centre (NNK) in 2023 and the new name of the authority is: National Health and Pharmacy Centre (NNGYK).

In clinical research, it is the responsibility of the investigator, principal investigator or investigating physician to obtain the prior consent of the participant. The data controller, typically the healthcare provider, is responsible for managing and processing the relevant health data. Prior notice and explicit consent of the data subject (Patient) needed. Data may be accessed for the purposes of scientific research[23] but no copies may be made of personal data.

In clinical trial, very considerable internal resources need to be devoted to so-called "serious adverse events" (SAE), which include the detection and reporting to the authorities of unforeseen events, injuries, symptoms and device failures during a clinical trial.

The above shows how more efforts are required for the proven applicability of an AI system in clinical research than for another AI system used outside of healthcare.

Within certain limits, social science research may also be performed, and it is not subject to such strict authorisation. In this respect, however, great care must be taken to distinguish what may constitute such a case, because if the device used turns out to be a medical device and the research constitutes medical research, then it is considered as clinical research carried out without authorisation, which is punishable under Article 171 of the Criminal Code as a violation of the rules governing research on human subjects, by imprisonment of 1 to 5 years.

Similarly, deviation from the authorisation is actionable under the same provision, and therefore special attention should be paid if the activity is not included in the study plan or documentation or if research is not performed precisely in accordance with it.

In clinical research, medical responsibility remains unaltered, whether it is for research into an artificial narrow intelligence (ANI) or another device. If the AI device controls the dosage of a product during some interventional trial, or even if it is implanted in the body and used in an invasive way in conjunction with or as part of a medical device, it is still the responsibility of the treating physician to monitor, and override if necessary, or stop the operation performed by such a system. This must be enabled by the developer. Otherwise, there will be no investigator who could responsibly perform the trial.

In the case of predictive AI systems, which give forecasts and calculate probability, and make recommendations that are difficult for the physician to control and follow, the following question arises. How liability should be handled in the clinical study? Firstly, the data subject should be provided with disclosing and understandable information about the risks arising from the operation of the system and consent should be sought. Failure to do so should clearly be the responsibility of the physician. Secondly, all the possible avenues of redress between the developer and the healthcare provider should be regulated in detailed contracts, and separate supplementary liability insurance should be taken out in such cases.

Ultimately, if an injury occurs despite the strict authorisation and monitoring of clinical research, the Government will compensate the patients or their relatives if the research had been carried out in accordance with professional rules and the research protocol. However, the ability to pay damages and compensation must be covered by compulsory liability insurance by the healthcare provider conducting the research.[24]

Clinical research carries the highest risk for healthcare – even without the use of an AI system, since the basic aim of research is to improve diagnostics, treatment, prevention and rehabilitation by intervention or observation, and by deviating from the usual healthcare practice.[25] According to Article 164 of the Act on Healthcare, "the interests of the subject always prevail over the interests of science and society in research", the law endeavours to settle an ethical problem. The conflict of interests is an ethical issue among the patients, society and science.

It is in the patient's interest to get cured and stay healthy. It is in the interest of society to have as many healthy people as possible within the limit of a social insurance budget. It is in the interest of science to make scientific progress and to present it. The legislator is of the opinion that the interests of the patient

[23] Health Data Protection Act (1997. évi XLVII.), Section 21.

[24] Based on the obligation imposed on the Member States under Article 69 MDR, and regulated by Articles 163-164 of the Act on Healthcare.

[25] Article 157 of the Act on Healthcare.

concerned, i.e. the trial subject, are the most important, and everything else must be subordinated to this. In practical terms, therefore, a healthcare AI system must be developed in a way that it should put the patient's interests first in decision-making situations.

Clinical trials controlled by government authorities enable that new technology remains safe and allow people to trust in new technology improvements. Clinical staff and service providers need to trust in the medical devices which therefore must be transparent.

5. ***Transparency and trust***

It seems that people have trust in certain online medical systems, especially if systems are controlled by the government. They believe that controlled medical systems must be accountable. Transparency is the hallmark of accountability. Transparency in terms of technical context means that an expert can translate (interpret) from the input and output data of the code what operations the machine performs in the computational process between the two endpoints and why it comes to this conclusion.[26] Transparency encourages people to trust in technology.

Like independently from the epidemics, in the age of information society people first look for information available on the Internet when they have a problem to be solved. Confirmed by research, more than 70% of the Hungarian population uses the Internet in connection with their health issues.[27] According to the survey, sources of information were websites, social media, patient groups (on Facebook), blogs, podcasts. Apart from that the professional literature was not easy to access, participants in the survey also could get information from the medical journals. This is why the initiative to rate patient websites regarding transparency and professionalism was commendable.[28] Why medical journals are closed in front of the wider audience? Professionals say it is because giving information for individuals should depend on the current type of personality, the diagnosis, the health status of the patient, and therefore must be given by a physician.

The e-patient phenomenon involves cultural and social transformation. According to research,[29] a large majority of the healthcare community is aware of and would like to use the technology, which can be found at medical conferences, literature and trainings.

However, according to the survey, there is a significant segment (18%) who do not use telemedicine solutions at all. Projecting doctor-patient survey data onto each other, it could be seen that one-fifth of the patients feel that their doctor was not in favor of searching for information on the Internet. They felt this well, while one-sixth of the doctors indicated that they were opposed to finding information about patients on the Internet. Nevertheless, there were examples of well-managed medical groups on Facebook, like the practical information on non-medical, yet care-related practical information, office hours, holidays, prescription order.[30]

The vast majority of doctors were happy to use remote consultation regardless of the pandemic.[31] In Hungary, the Single Health Database Processor (EESZT) was introduced in 2017 by the Hungarian Government.[32] The spectacular results of the EESZT systems were to spread and generate 800.000 recorded e-prescriptions on a daily basis, yearly 75 million medical reports, and documented 180 million doctor – patient meet.[33]

The e-recipe has almost completely substituted the traditional method of writing recipes. Even in case of a personal visit, the doctor does not print the prescription, or the patient receives a reminder sheet summarizing the medicines, which he can present at the pharmacy and put away for him or herself.

[26] G. Magyar and A. Nemeslaki, *Technical Questions of Digital Transformation,* Budapest, Gondolat, 2021, 175.
[27] E. Girasek, J. Boros, B. Döbrössy, A. Susánszky and Zs. Győrffy, *E-patients in Hungary.*
[28] J. Ködmön, *Healthcare information on the Internet,* in *Medical Journal (Orvosi Hetilap)*, 2018, vol. 159, no. 22, 855–862.
[29] E. Girasek, J. Boros, B. Döbrössy and Zs. Győrffy, *E-healthcare Service in Hungary: Digital Healthcare Experiences and opinions of local doctors,* Semmelweis University, Medical Sciences, Behaviour Department, Budapest, in *Medical Journal (Orvosi Hetilap)*, 2023.
[30] S. Balogh and E. Diós, *Hómofisz. Case Study of Two Weeks in a GP*, Medicus Universalis, LIII. ÉVFOLYAM 2. SZÁM, 2020.
[31] R. Kránicz, A. Hambuch, R. Halász, L. Makszin and A. Sárkányné Lőrinc, *Study of the telecommunication and consultancy in GP and Specialits Service Providers*. Pécs University, Medical Sciences, Public Health and Communication Institute, Bioanalytics Department, Porta Lingua, 2022, 2.
[32] https://hu.wikipedia.org/wiki/EESZT
[33] E. Girasek, J. Boros, B. Döbrössy, A. Susánszky and Zs. Győrffy, *E-patients in Hungary.*

Is there any legislation that demonstrates what makes a code interpretable? Would the algorithm become transparent if the code was published? Is ethical design simply the economic interest of the developers to build trust in their product?

A recent study could be the answer of trust building, how a system could be 'trustworthy'. The first step in such a "human-centered design" is to define the clinical task that the machine had been intended to support and to examine the existence of the personal and material conditions required by health regulations.[34]

It is necessary to determine the characteristics, features, accuracy, explainability, interpretability of the algorithms to be used. It is equally important to understand the capabilities and responsibilities of future device users. According to the study, the second step is to develop an acceptable level of assurance and transparent devices for the user (medical staff).

Without such a design the device will not be used or will not be allowed to use. If developers do not go along that lines, they can't sell their product. In the next steps, it must be ensured that what was laid down at the beginning of the rules will be followed by the model throughout. This should be demonstrated to the user, appropriate measures (metrics) should be linked to the evaluation of the performance, and finally, whether the built-in transparency tool is effective (validation). The latter rule also increases acceptance, it has a direct impact on the economic result of development.

Another study based on the AI-HLEG[35] guidance also emphasizes the importance of co-design for the reliability of a skin lesion testing system.[36] It is recommended to involve not only the physician, but also the patient. It is recommended to perform a distortion of the training data by ensuring the diversity of the database elements. The results should then be presented according to standardized requirements for the transparency of the study (TRIPOD, CONSORT-AI, MINIMAR[37]).

There is also a legal basis for accountability. According to the MDR, the developer must have up-to-date technical documentation, prepare an EU declaration of conformity, ensure compliance with the standards through a quality management system during serial production. The quality management system must guarantee the requirements of safety and performance. Managerial responsibilities include the requirement of supply chain supervision, follow-up and surveillance system, serious incident reporting (SAE) in the context of vigilance.[38]

Building trust in technology is in the interest of both the developer and the healthcare service providers, and patients are who enjoy the benefits. Though patients must be protected against unlawful and malicious practices.

6. *Data Privacy*

Data Protection Authority discovered breaches of data subjects' rights. Like the National Authority for Data Protection and Freedom of Information found unlawful the practice of an AI backed solution and fined a bank for 250m HUF, which used AI solution to evaluate call centre conversations but had not given any notice to the client in advance.[39] In other cases the Authority ordered to provide patients records for free as it is their right to access to data.[40] These shows how important is for the data controller to comply with law when using AI or processing health data. There has not been published any cases yet when controller breached the law related the use of AI on health data.

Due to the nature of the AI, the largest possible dataset is required to get trained on an AI medical device. As the issues related to AI and data protection constitute an important and wide-ranging topic, due to their

[34] H. Chen, C. Gomez and C.M. Huang (eds.), *Explainable medical imaging AI needs human – centered design: guidelines and evidence from a systematic review*, in *Digital Medicine*, 2022.

[35] European Commission High Level Expert Group on AI, 2019.

[36] R.V. Zicari *et al*., *Co-Design of a Trustworthy AI System in Healthcare: Deep Learning Based Skin Lesion Classifier,* in *Frontiers in Human Dynamics*, vol. 3, 2021.

[37] TRIPOD-AI: *Transparent Reporting of a multivariable prediction model for Individual Prognosis Or Diagnosis*, 2015; CONSORT-AI: *Consolidated Standards of Reporting Trials,* 2010; MINIMAR: *Minimum Information for Medical AI Reporting.*

[38] MDR, Article 10.

[39] National Data Protection Office (NAIH), case no. NAIH-85-3/2022.

[40] NAIH, case no. NAIH-3849-16/2022; NAIH-4137-8/2022.

voluminous nature. There are many phases of the development like collecting data, building model, developing the application, and therefore they arise many questions, especially regarding the data. Like where to obtain a large number of data? Is the database structured? Does it comply with data protection principles and the requirement of equal treatment?[41]

Having the Single Health Database Processor on board (EESZT) it should have a huge advantage over other Member States of the EU or even large States on other Continents where they have units divided into more social insurance funds and service providers. The only instrument is missing from the process is a 'regulatory sandbox' for start up companies to get health data and build their models and applications. Without start up ecosystem in healthcare, the government should develop technology on its own, and start up companies will move to other countries where they can have health data sets. Without having medical start up companies, only tech giants will in a position to offer services and products using AI powered technology.

So, if there is data, machine learning systems will be developed in healthcare. Data in paperwork are not digitized and not structured, and developers need digital datasets. In many cases still the nurses administer manually the temperature chart. Technology[42] could replace the fever plate with sensor technology placed on the patient's wrist. During COVID, vital measurements could have been recorded contactless, which could be automatically uploaded to the hospital information system (HIS), freeing nursing staff from administrative burdens. However, it must also be seen that institutional infrastructure needs to evolve for this, for example in the areas of data transfer capability and speed, storage capacity, information security.

The quality and quantity of data is essential for the AI, without which the AI cannot work. In technical terms, it is important that the data is as easy as possible to process, i.e. structured and organised. For machine learning purposes it needs to be effective, it is important for the AI to have a large amount of correctly recorded, complete data. From a legal and ethical point of view, it is also important to comply with data protection requirements and to ensure that the database is fairly composed and compiled without discrimination (fair database).

A database that is anonymised, i.e. made available in a way that does not identify the person concerned, is less valuable. Data that can be continuously monitored and linked to the subject, reflecting the current health status of the person concerned (subject), is much more valuable in healthcare AI system. The information of the case history, the medical history, the lifestyle shows the lifecycle of the Patient, so the research into diagnosis, the prevention and the therapy for the present and future can be monitored.

It is often not possible to foresee at the time of admission what still needs to be examined in the process of treatment, from the detection of the disease to recovery, so the data hardly can be shared in many cases.[43]

The GDPR defines a data subject only in terms of personal data,[44] while the national law[45] defines a data subject as "any natural person identified or identifiable on the basis of any information".[46] By invoking the concept of a data subject in the Health Data Protection Act, one comes to the concept of a healthy or ill natural person, specifically created or arising in relation to the use of healthcare services.[47] The concept of health data is also regulated by the GDPR,[48] and it is supplemented by Article 3/A of the Health Data Protection Act, which states that EU rules also apply to the health data of deceased persons. In the course of healthcare provision, the personal data that are not considered as sensitive data and that serve to identify the data subject, such as name, address, birth data, identification numbers, social security number, may be processed as part of the

[41] As defined in Article 7(1) of the Act on Healthcare.
[42] www.entremo.com.

[43] C. Watson, *Many researcher say, they will share data, but don't*, in *Nature*, vol. 606, 2022, 853.
[44] Article 4(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereinafter "GDPR").
[45] Act on the Right to Informational Self-Determination and Freedom of Information (CXII of 2011).
[46] Article 3.1 of Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information.
[47] Article 2.b of Act XLVII of 1997 on the Management and Protection of Health Data and Related Personal Data ("Health Data Protection Act").
[48] Article 4(15) of the GDPR.

medical records pursuant to Article 3/B of the Health Data Protection Act. From the perspective of AI, the essence is that personal data and special health-related sensitive data are any information, information detail, data fragment, indirect data stream or derived data, which can be linked to the data subject, no matter how distant the correlation is.

The developer, the operator of an AI system must comply with the statutory requirements for the exercise of rights by the data subject. The relevant literature classifies data subjects' rights along the lines of transparency and accuracy as the basic principles of information self-determination.[49] The right to prior information, the right of access and the right to data portability serve to enforce the principle of transparency. The data subject's rights to rectification, erasure (right to be forgotten) and restriction of processing are rights that help to enforce the principle of accuracy. The third group is made up of the other rights set out in the GDPR, such as the right to object, and the prohibition of automated decision-making.

The responsibility of data controllers starts with respect for the data protection principles of lawfulness, fairness and transparency; purpose limitation, data minimisation, accuracy, limited storage, integrity and confidentiality, and finally, accountability.[50] Already at the development stage the manufacturer of the AI application should consider how the institution or healthcare provider that will use the system will be able to comply with the data protection requirements. The requirement of data protection by design is the responsibility of the data controller. So there are legal requirements on data privacy, on medical devices and developers also need data to train, to test and to validate an AI system.

Imagine the burden put on healthcare start-ups comparing to other industries! Developers than need to comply with EU, US, Middle East, Far East, Australian and other data protection regime as well if they want to roll out their activity out of the national market. For a "Tech Giant" this is obviously just another compliance task, but for a start-up it is a barrier to market entry, which is not even realised by developers at the time of launching the business. A global harmonisation of rights and obligations in relation to health data could have a huge cost-reducing effect on the spread of AI in healthcare, and it could start with epidemics, as the control of epidemics is in the global and individual interest of all existing states at the same time.

A prior (in this context: data protection) impact assessment by the data controller is certainly required when an AI application is introduced for specific data processing handled by an institution or service provider in healthcare, which inherently constitute high-risk data processing.[51]

It is also a fundamental obligation for the controller to take appropriate technical and organisational measures under Article 24 of the GDPR. It is the data controller's responsibility to maintain up-to-date records of the processing, and to remedy and report any data breach. Such obligations may lead to unresolved liability situations and disputes in the case of insufficiently thorough arrangements between joint data controllers or a data controller and a data processor. For this reason, in the course of selling the AI application, the developer or manufacturer of the AI system should take particular care to ensure that the roles and responsibilities of either the joint controllers or the data processor are as clearly defined as possible. In any case, the procedural protocol to be followed in the event of an incident should be specified and a time limit should be set. It is worth for the AI developer/manufacturer to strive for processor status (as opposed to the quality of joint data controllers), arguing that the healthcare provider is the data controller, and this determines the purpose and method (tool) of data processing, while the AI only facilitates the technical assessment of the data, and the decision is made by the data controller. The data controller is also responsible for the adequacy of the choice of the data processor under Article 28(1) of the GDPR, and thus if the developer or manufacturer of the AI can present its GDPR compliance to the future data controller in advance, it may facilitate the marketability of the AI application in the EU.

The right referred to in Article 22 of the GDPR is in fact a prohibition, since according to the original wording, the data subject "shall

[49] A. Péterfalvi (ed.), *Explanation of the GDPR,* Wolters Kluwer Hungary, 2018, 149.
[50] Article 5 (1) and (2) of the GDPR.
[51] A. Péterfalvi (ed.), *Explanation of the GDPR*, 231.

have the right not to be subject to" a decision based solely on automated processing, including profiling, if it produces legal effects concerning him or her or similarly significantly affects him or her.

An exception to this rule is where the decision is taken for the performance of a contract between the data subject and the data controller, or on the basis of a legal provision, with appropriate safeguards, or on the basis of the data subject's explicit consent, and the data subject is given the opportunity to request human intervention in the decision, to express his or her views or to object. A further prohibition on special data is contained in paragraph 4 of the same Article, and it is also mentioned in preamble (71) that data concerning health status can only be based on explicit consent and on general public interest.

According to the national law[52] the medical staff can create a profile in the National e-Health Infrastructure Database (EESZT) for the patient including the identification numbers, status of patient, diagnosis, treatments, other records. In case of death the profile will be automatically deleted after 10 years retention period. The patient can request not to upload any information to the database. So it is still recommended to maintain the possibility for the data subject to object, and the possibility to facilitate the right to access, the right to be forgotten regarding data processing.

Data is essential for AI developments, and data protection is essential to keep patients fundamental rights. Healthcare decision makers though need to think about how to keep start up developers in the Country, in the EU and make health datasets available for them to collect data, build models, develop applications in a controlled environment.

7. *Machine Learning and Data*

Important concepts are the training of data, the test and the validation of them. The latter considered as data used to evaluate the AI system and to set the unteachable parameters and learning process. This issue is closely related to the regulation of special data management in the healthcare domain.

Imagine that a trainable AI application is developed in the field of diagnostic, which is supposed to demonstrate its ability to provide accurate, reliable, safe assessment of CT scans in the context of clinical research. Thus, the developer first needs a large amount of historical data to be able to form a data set from the image resolution, to develop appropriate screening conditions from the data set, to correctly evaluate the classification based on the screenings, and then to visualise the correctly classified data set in a way that can be evaluated and processed by the radiologist.

On the other hand, a healthcare provider, may acquire and store imaging recordings and manage them for data protection purposes. Thus, either retrospectively or during an ongoing clinical research, the developer should be involved in the institution's activities, either as a data processor or as a joint data controller, to access already evaluated findings and images.

Moreover, in clinical research, the actual and follow-up data is supposed to be the most important for science and development. Take for example the fact that the accuracy and image resolution capabilities of an AI application allow it to detect changes in a cancer patient's condition (tumour size) after the first or first few chemotherapy treatments. How could this be developed in clinical research without up-to-date data and without a real data subject, not anonymised but actively involved in the therapeutic treatment?

From a therapeutic point of view, this is important if a patient is treated with a pharmaceutical product for months and only then it is found not to be sufficiently effective or ineffective. This time is too long in view of the fact that after just one or two treatments it would be possible to decide whether the active substance is effective, or it needs to be changed. Think about the fact that with certain AI applications, we may be able to get the results in a way that is even more predictable after the test. In practical terms, it is psychologically stressful for the patient to be called back for a follow-up test after a screening test, and it is especially physically stressful for the patient to be subjected to a chemotherapy treatment that is ineffective for him or her but that has been going on for long months.

From a data protection perspective, it is a strategic issue to be able to train and test algorithms on data recorded in each health data space. Such as the Single Health Data

[52] Article 35/J of Act XLVII of 1997 on the Management and Protection of Health Data and Related Personal Data "Health Data Protection Act".

Processor (EESZT). The application developed in this way can then be extracted from the database and the now commercially viable AI tool can be used on live systems. To do this, the developer will otherwise have to overcome additional problems, for example, compatibility with certain imaging equipment, and to ensure that the trained tool works with the same accuracy in a standard environment.

Another strategic question concerns compliance with the provisions of the forthcoming AI code:[53] To what extent will this increase the costs of development, slow down progress or even be a barrier to the EU's health industry?

After all, from the investor's point of view, medical technology and pharmaceutical developments are the projects that carry the highest risks and the longest payback periods due to the specificities of clinical research and authorisation. If this area fails in the market, then an intervention will be required at the level of the EU as well as the Member States to offset the increased costs that Europe will incur. Such may include, for example, the setting up of funds specifically earmarked for supporting R&D, tax incentives, EU or national guarantees, or even measures such as allowing access to a single, controlled but freely searchable and structured data set.

There is a risk of selling one's health data[54] because poorer people would be forced to sell their data, making them less able to protect their data other than the rich. However, who wouldn't give away everything, including the health data, to be cured, or to find the right cure for a family member? In the public interest, the concept of 'data solidarity' already exists in the EU.[55] On a non-profit basis, companies may collect personal data without the consent of the data subject. This may even lead to a grey zone, because the range of data controllers can easily change, and related products are already expected to enrich the business sphere during data management.

The example to follow could be the "Next Generation Medical Infrastructure Law"[56] in Japan, which allows hospitals to transmit health data to accredited companies with patient consent, which anonymizes it and makes it searchable. The EU would also like to set up such data hubs.[57] Patient Society has already started such a recruitment to build databases. For example, when people suffering from the same disease or group of diseases, they share their data for the sake of science and research.[58]

Data processing is ethical and lawful if the patient has freely consented to its processing on the basis of prior information and the data has been used for what he or she has consented to. The question is, should health data be protected as part of the private sector and therefore should not be allowed to benefit from it? Or is the individual's health data the value of the human community, through which many other people can be healed, so it should be used and utilized for the benefit of the community? Or should we leave the decision of the question to the individual freely, so that the data can be traded at the discretion of everyone, and whoever puts it up for sale should bear the consequences of their risk and benefit from it?

The strategy has therefore not yet been decided in the area of data sharing. We emphasize that this is not about data in general, but about health data, the knowledge base of which can help the patient, his relatives, fellow human beings. Technology could also provide an answer to this, for example, blockchain could allow all three trends to prevail at the same time. It could be used anonymously, yet even at the same time, allowing trading (utilization), it would work in the interest of the community. Blockchain technology can solve the privacy issue of the data controller having to share health data with other data controllers. Yet learning through data can take advantage of technology and only the results of testing are shared between the institutions in the network.[59]

[53] 2021/0106 (COD) Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts.

[54] WHO Guidance, *Ethics and Governance of Artificial Intelligence for Health*. Geneve, World Health Organization 2021, CC-BY-NC-SA 3.0. IGO, 76-82; Annex, 141, 84.

[55] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act).

[56] WHO Guidance, *Ethics and Governance of Artificial Intelligence for Health,* 83.

[57] Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space.

[58] https://datasaveslives.eu; www.datafair.org; www.registratieaandebron.nl.

[59] S. Warnat-Herresthal *et al*., *Swarm Learning for decentralized and confidential clinical machine learning*,

The need for the health data is growing. It is very difficult for a startup developer to get it. When planning an AI development, it is advisable to make sure in advance from which institution, what patient data, under what conditions can be collected and processed.

8. *Liability for AI systems*

The health legislation itself is very diverse, a recurring legislative reference to the application of directives, professional and ethical rules when determining the appropriate level of care. Thus, in addition to the various levels of legal provisions, the right decision must also be made in the maze of ethics rules, national and local level, different institutional guidelines, and protocols. [60] Doctors often complain that while they must make the right decision within minutes, there are years for high level professionals, legal and forensic staff to establish the responsibility or exempt.

These professional rules, guidelines and protocols can be converted into programmable decision trees and can be queried quickly and easily with the help of an AI system. This still does not mean that a doctor is exempt from responsibility if a machine were to tell what professional rules apply. If this system is trained with continuous feedback, like a conversational assist, a telemedicine application for doctors can be developed by using a machine learning method. Benefits would be to know how others decided in similar cases, what the outcome was, what questions others asked and what else they were curious about.

The final decision, the responsibility for the decision, is always on the doctor. So, the AI system does not replace medical intelligence, but rather an extended intelligence, the intelligence of common medical knowledge and experience. Doctors must understand the logic of the system and its limitations. The institution must implement the system properly, constantly monitoring it in accordance with the documentation.

8.1. *Liability of the developer*

As a result of successful clinical research, the developer gets an assessment of the AI device. The healthcare institution then can buy it and put it into circulation. This creates a contractual relationship and a related contractual liability regime in relation to the product sold.

The developer is liable for defective performance in accordance with the rules of breach of contract in accordance with Section 6:157 of the Civil Code[61] if he does not meet the quality requirements specified in the contract or by law at the time of performance. Based on his or her warranty rights, the injured party may request repair, replacement, and price reduction at his or her option. Alternatively, the developer could have someone else repaired the product, but since it is essentially software, even if the user obtained the source code, it would be impossible for someone else to repair it.[62]

Wearables should not be confused with wearables or invasive implanted devices ordered by a doctor, which are naturally certified in clinical research and approved by the authorities for therapeutic and diagnostic purposes.

The knowledge and scope of use of the two types of devices (wearables and medical devices) will probably get closer and closer to each other. One will learn from the other area. So, the demarcation will also become more and more difficult for licensing and legal judgment. The smart device is not a medical device, but it can provide a lot of very important data to the doctor. Data can be sent even through a telemedicine application in advance to the doctor. At the end, doctors are obliged to examine the patient in all cases independently what he/she had received in advance.

What if AI is only one component of the product, is the responsibility separated of the manufacturer regarding the hardware and the software? From the user point of view (hospital), it is certainly not, unless they are separate suppliers by contract. However, if there is a CT scan product, which is sold in conjunction with an imaging diagnostic AI system and which acts as a user system, the parties are contractually advised to settle their liability in a detailed contract, to the extent of it, and how to settle a dispute.

8.2. *Hospital's liability*

In the legal relationship between the institution and the patient, the doctor decides on the diagnosis and treatment since the AI

in *Nature*, vol. 594, 2021, 365.
[60] Act on Healthcare, Section 7 (2); 77 (3).
[61] Civil Code (2013. évi V.).
[62] Civil Code 6:159 §.

system currently only complements medical intelligence and facilitates the processing of information.

The mandate contract or an atypical "medical treatment" contract is concluded between the healthcare provider (hospital) and the patient.[63] The Act on Healthcare Section[64] 244 provides clear guidelines for the establishment of liability for damages, because according to subsection (2), the rules of the Civil Code on penalties for non-contractual damages and violations of personal rights apply. Who is liable on the care provider's side, as follows from paragraph 1, is the responsibility of the healthcare provider for damage caused in the context of institutional care and for violations of privacy and rights relating to personality.

In practical terms, therefore, the legal relationship between the hospital and the patient, or between the doctor and the patient acting on his own behalf, is governed by the contractual rules of the Civil Code, except in terms of tort, where the rules of tort liability shall be applied.

Section 6:519 of the Civil Code applies to the liability rules for damages without any contractual relationship. Anyone who unlawfully causes damage to another person is obliged to compensate. In connection with the involvement of the AI system, anyone who makes a claim for damages against the user of the system, i.e., the supplier, the doctor, and even jointly and severally the developer or manufacturer, must prove the unlawful tortious conduct, the occurrence of the damage and the causal link between the tortious conduct and the damage. The other party must prove that its conduct was not attributable to be exempted.

In the doctor-patient relationship, there is an information asymmetry that the legislature is trying to counteract in a lawsuit on the side of the injured patient. Such provisions include an obligation on the part of the respondent provider to provide information in the event of a statement emergency under Section 170 Subsection (5) Point (a) of the Civil Court Proceeding Act,[65] or the mandatory attachment of the means of proof in an evidentiary emergency under Point (b). When using the AI system, this information asymmetry can be further pushed back on the side of the supplier, and the supplier must even consider to be able to fulfill its obligations in this direction in a lawsuit. Thus, the developer, manufacturer, third-party operator of the AI system should provide the information or evidence.

For example, if, during an imaging diagnostic analysis, both the radiologist and the AI do not recognize the lesion, even though it was recognizable, it is an unlawful tortious behavior. The patients lose their chance for a speedy recovery or there is a deterioration in their health, they lose the earning capacity, there are costs for the care, this is the harm to the patient. If they had recognized it in time and started treating the patient, there would be no deterioration in the patient's condition, this is the causal relationship between the caregiver's behavior and the damage.

In order to be defensed, the health care provider must prove that the Healthcare Act Section 7 Subsection (2) he or she acted in accordance with the current professional and ethical rules and guidelines and with reasonable care, at the time of making the diagnosis, he or she could not have foreseen from any data, signs or information that the disease was developing, there was no reason to obtain another medical opinion, to request a consultation, or to recall the patient for control.

8.3. *Violation of personality rights*

According to Section 2:52 of the Civil Code, damages may be claimed from the infringer for violations of his personal rights in accordance with the rules of liability for damages caused unlawfully. Such a grievance fee may be claimed in connection with an AI system. For example, in relation to the right to inadequate and unindividualized information, where an AI-driven communication takes place in it. The same as in relation to a breach of the right to access the medical records of the patient, or if the data in the database used by the AI is lost, or the medical secret may also be breached, in the event of inadequate protection of such a database.

8.4. *Criminal Offence and Infringement*

In connection with the AI system,

[63] B. Kórodi, *Litigation emergencies in lawsuits for disadvantages related to health services,* in *Hungarian Legal Journal (Magyar Jog)*, 13 January 2020.
[64] Act on Helathcare (1997. évi CLIV.)
[65] Civil Court Proceeding Act (2016. évi CXXX.)

falsification of a health product within the meaning of Section 186 of the Criminal Code[66] can be considered by the implementation of a factual situation. Also, crimes committed in the context of an occupation where the AI system is used during the crime. Staying with the health product, by definition, a medical device falls within this category, and if not, the criminal conduct that falsifies the AI system itself, but its documentation, or is not allowed to be placed on the market or even to possess such a product, the facts of the case are realized and are punishable by imprisonment for up to three years. Health breach liability in connection with the AI system may arise, for example, in the case of false statistical reporting if the data processing is carried out using such a system.

8.5. *Market surveillance*

Chapter VII of the MDR provides for a post-market surveillance system that regulates the manufacturer's obligation to self-monitor and follow-up. The competent authority in Hungary is the National Institute of Pharmacy and Nutrition.[67] Thus, within the scope of the general control and supervision activities of the authority, the MDR market surveillance system is based on documentation testing, laboratory testing of sampling, conformity testing of devices, vigilance and complaint reports. It shall also carry out checks on the product of the manufacturer, importer or distributor in an individual market surveillance system in accordance.

Further actions can be taken with the help of consumer protection, for example with regard to wearable smart devices, may arise if an AI system is used by the service provider.

An infringement of advertising law or unfair market conduct may be considered if the promotion of the dissemination or use of the AI system conflicts with some prohibited advertising or is carried out in a way that influences the consumer through fraudulent means.

The data protection authority is key to the availability of data in relation to the AI system. The data subject will not have confidence in AI systems where data protection is inadequate, this lack of trust may even be a barrier to the development of the AI industry.

8.6. *Patient's complaints*

From the patient's point of view, what can be done to enforce patients' rights if they have a complaint during care? For example, he feels the AI technology used has not served his/her interests. Many patients need direct medical contact, and he/she is not happy when, during care, the doctor is pushing machines, staring at a screen and looking as if he does not care about the patient.

In many cases, the patient complaint is emotionally overheated, and in the event of the loss of a relative, the unprocessed grief drives the patient as a motivating force. The patient has the opportunity to complain to the care institution, it is possible to turn to the patient's representative for the patient's rights, to use the mediation advice and to take the dispute to the legal path.

The patient can also complain to various organizations.[68] Based on the complaint, the determining medical authority[69] exercises professional supervision and acts in accordance with the General Administrative Order (AKR), its sanctions may be warning, downgrading, suspension, withdrawal of license, imposition of fines.[70]

8.7. *Liability Insurance*

Through compulsory liability insurance in the field of healthcare, the compensation capacity of the provider and doctor operating in the care system is established. However, during the operation of an AI system, where there is necessarily a lot of patient diagnostics, a lot of therapeutic treatment, a lot of data management, even the highest amount of insurance available on the market may be scarce for coverage, so it is recommended to use additional insurance.

What happens after the cessation of activity? For example, the given AI system is outdated, it is disconnected, the product is no longer supported, but the damage happened earlier. The "Long Tail Liability" is becoming aware after a very long period of liability

[66] Criminal Code (2012. évi C.).
[67] Országos Gyógyszerészeti és Élelmezés-egészségügyi Intézet (OGYÉI) – after changes in 2023: (NNGYK).
[68] Chamber of Ethics Committee, OGYÉI, NEAK, NNK.
[69] Healthcare Act Section 123.
[70] Act on General Administration Procedure (2016. évi CL.).

enforcement and insurance liability even beyond the limitation period. It is therefore appropriate to expect that liability insurance will be maintained for an even longer period of time in order to mitigate the risk.

millions of lines, but so that we can explain how it works, and in case of doubt we can decrypt the causal chain in a documented way, finding the root cause of the problem.[71]

9. *Other achievements*

There are other achievements in digital healthcare. Like the National Ambulance introduced the 'Lifesaving Coronavirus' application.[72] Communication can help not only those involved in emergency care, but also those working in care in general. For example, through a specialist psychological emergency call service, you can manage the workload, burnout, depression, and psychological burden of individuals. Patients also feel the weight of this on the other side, and balanced service at the bedside increases the patient's sense of security, satisfaction, and thus the chances of recovery.[73]

There have also been COVID-induced developments in the wider healthcare system. For example, in wastewater-based epidemiology to predict the spread of the virus, algorithmic analysis was used to show the relationship between virus concentration and case count in wastewater using linear regression.[74]

In the field of infection control, not only developments are related to data processing, closing disinfectant cleaning to prevent COVID and other infections was carried out with non-contact surface disinfection technology, especially where units with high infection rates are located.[75]

Data-based clinical research is important according to the recommendation of the Health Science Council (ETT) because multicentre data collected online are collected in a structured way, making it easier to improve the efficiency of treatment through its analysis, and with the new concept of translational medicine, research on anti-COVID agents is a good example of the repositioning of previous pharmaceutical products.[76]

10. *Conclusions*

Declaring that COVID19 accelerated the development of digital toolkits in healthcare, the study assured that the proper legislation was evolved to use new healthtech achievements. The majority of doctors and patients are happy with the technology, so this trend is expected to spread further in the future. The study pointed out that patients accepted the new technology in general, though there are still some concerns for certain groups of people living with disabilities or in poor living standards or the lack of education becomes an obstacle. The current legislative system has clear definitions on medical devices. Both patients and clinical staff trust in systems as long as the technology is validated in clinical trials. Future prospects like the AI Act requires further risk assessments of medical systems.

The study showed that building trust in technology is in the interest of both the developer and the healthcare service providers, and patient is the one who enjoys the benefits. At the end, patients still must be protected against unlawful and malicious practices, like in any data protection incidents.

The need for the health data is growing. It is very difficult for a startup developer to get it. When planning an AI development, it must be clarified which institution, what patient data, under what conditions can be collected

[71] C. Bartneck (ed.), *An Introduction to Ethics in Robotics and AI*, Springer Briefs in Ethics, Cham, Springer, 2021, 36,37.

[72] Z. Győrffy (ed.). *Telemedicine During COVID-19 in International and Hungarian experiences and guidelines,* in *Medical Journal (Orvosi Hetilap)*, 2020, no. 24, vol. 161, 983-992.

[73] T. Irinyi, A. Németh, *Burn out and depression in the medical staff* , Study, Elitmed, 2022 https://elitmed.hu/kiadvanyaink/nover/kieges-es-depresszio-az-egeszsegugyi-szakdolgozoi-tarsadalomban/pdf-open.

[74] T. Pándics, E. Róka, J. Henczkó, B. Khayer, Z. Kis, T. Málnás, B. Pályi, E. Schuler and M. Vargha, *National forecast system on COVID-19 predictions using rest water – conclusions of 1,5 years,* Public Health Journal (NÉPEGÉSZSÉGÜGY a népegészségügyi képző- és kutatóhelyek országos egyesületének tudományos folyóirata, 99. évfolyam 1. szám.), Semmelweis University, Health and Technology Analytics Centre, 2022.

[75] I. Kopcsóné Németh, Cs. Dandárné Csabai, O. Bazsó, M. KÄFER, Zs. Biró Zs., M. Balogh, M. Csák and O. Csordásné Gergely, *Hospital infection controll during COVID-19, prevention of MRK infections in Honved Hospital,* Public Health Journal (NÉPEGÉSZSÉGÜGY a népegészségügyi képző- és kutatóhelyek országos egyesületének tudományos folyóirata, 99. évfolyam 1. szám.) Semmelweis University, Health and Technology Analytics Centre, 2022.

[76] ETT Guideline no. ETT IV/8537/2021/ETT.

and processed.

The final decision on the diagnosis, therapy and the liability for the decision remains on the doctor. So, the AI system does not replace medical intelligence, but rather it extends the intelligence, in the sense of a common medical knowledge and experience. What medical staff can do? Doctors must understand the logic of the system and its limitations, while the hospital must implement the system properly, constantly monitoring it in accordance with the given documentation.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 87-139
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 08

*Public Procurement of AI for the EU Healthcare Systems. First Insights from the Spanish Experience**

María Estrella Gutiérrez David
(Associate Professor of Constitutional Law at Universidad Complutense de Madrid)

José Luis Quintana Cortés
(Lawyer. Partner of Rodríguez Castaño Abogados)

ABSTRACT Based on a sample of 20 selected tenders, this paper analyses the public procurement of AI solutions for healthcare systems, providing insights into the why (public need), the what (domain of application of AI) and the how (innovation strategies, procurement procedures, safeguards in tender specifications to ensure trustworthy AI).

1. *Introduction*

Healthcare services constitute one of the most important economic sectors in Europe, accounting for almost 10% of GDP, and 15% of government expenditure. A large number of investments are focused on the digital transition in healthcare (e-Health), including telemedicine, amounting approximately to EUR 12 billion.[1]

Looking ahead, the adoption of a regulatory proposal to create the European Health Data Space ("EHDS Proposal")[2] is expected as one the key priorities of the European Commission in the area of health. The purpose of the EHDS is to promote health-data exchange, support digital-health services and research on new preventive strategies, diagnosis and treatments of diseases, medicines, medical devices and health outcomes. Not by chance, along with its primary use, the EHDS Proposal also envisages the processing of electronic health data for secondary purposes, *inter alia*, "training, testing and evaluating of algorithms, including in medical devices, AI systems and digital health applications, contributing to the public health or social security, or ensuring high levels of quality and safety of health care, of medicinal products or of medical devices".[3]

In recent years, contracting authorities of the EU National Healthcare System (NHCS) have been engaged in the purchase of Artificial Intelligence (AI) solutions to tackle the challenges of the 21st century healthcare.

Procurement notices published by EU contracting authorities on digital platforms or buyers' profile show that this trend will continue and increase in the future. The extent to which this is the case remains opaque,[4] as there is no clear map of public purchases of AI solutions.

To address this challenge, this paper seeks to draw a first systematic picture of the current state of public procurement of AI solutions for

* Article submitted to double-blind peer review.
This paper is part of the research project "Artificial Intelligence in the national health care system: solutions to specific legal problems" (PID2021-128621NB-100), directed by Dr. José Vida Fernández and founded by the Ministry of Science and Innovation of Spain (MCIN/AEI/10.13039/501100011033/) and by "FEDER: A way of making Europe".

[1] European Commission, *Recovery and resilience scoreboard. Thematic analysis Healthcare*, December 2021, 3-4, https://ec.europa.eu.

[2] See Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space (COM/2022/197 final). Article 1(1) of the Proposal defines the EHDS as a data space "providing for rules, common standards and practices, infrastructures and a governance framework for the primary and secondary use of electronic health data". In general, "Data Spaces" are common and interoperable infrastructures that bring together (i) the deployment of data sharing tools and services for pooling, processing and sharing of data by an open number of organisations, as well as the federation of energy-efficient and trustworthy cloud capacities and related services; (ii) data governance structures which determine, in a transparent and fair way, the rights of access to and processing of the data; (iii) improving the availability, quality and interoperability of data – both in domain specific settings and across sectors. See also European Commission, *Common European Data Spaces*, SWD(2022) 45 final, Brussels, 23 February 2022.

[3] Article 34.1(g) of the EHDS Proposal.

[4] M. Hickok, *Public procurement of artificial intelligence systems: new risks and future proofing* in *AI & SOCIETY*, 2022, 1, 7. https://doi.org/10.1007/s00146-022-01572-2.

the NHCS in Europe with a special focus on Spain. In the context of the Spanish research project PID2021-128621NB-100, funded by the Ministry of Science and Innovation of Spain and FEDER funds, this contribution will try to provide some valuable insights into:
1) the *why*: the public needs to be met and challenges to be solved;
2) the *what*: the applications of AI and use cases, and;
3) the *how*: the procurement procedures implemented and, if any, the specific tender requirements to ensure appropriate safeguards to address the inherent risks of the use of AI in the NHCS.

2. *The context*

Particularly after the COVID-19 pandemic, public-healthcare systems have come under the spotlight due to the digital transformation. E-Health applications, including AI-based solutions, are starting to facilitate a holistic approach to health.

AI techniques, such as Machine Learning, Deep Learning or Natural Language Processing ("ML", "DL" and "NLP", respectively) have a very wide field of application. They can be used to improve the quality, efficiency and equity of national-healthcare systems ("NHCS").[5]

As a data-driven technology, AI has many potential applications to reduce uncertainty in medicine, and more specifically, in classifying patients' conditions (diagnostic uncertainty), in explaining why and how patients develop specific diseases (pathophysiological uncertainty), in determining the most appropriate treatments for them (therapeutic uncertainty) or in assessing the results of a specific treatment (prognostic uncertainty).[6]

In particular, AI can be used in public-health systems to discover new drugs, interpret X-ray images, or understand the progression of a disease and perform early diagnosis.[7] For example, during the COVID-19 outbreak, ML models were proposed to improve systems for triaging patients to the most appropriate services –for example, Intensive Care Units "ICU"– based on severity predictions.[8]

AI can also play an essential role in analysing and processing health data through the implementation of Electronic Health Records ("EHR")[9] or wearable devices and sensors via the Internet of Things ("IoT").[10]

Furthermore, AI models are being used to predict costs by private insurers, non-profit hospitals or governmental agencies,[11] and to optimise available healthcare resources by encouraging the automation of repetitive tasks.[12]

The pandemic has been nothing more than a catalyst for the design, deployment and acquisition of AI solutions by national-health systems.[13]

---

[5] E. Harwich and K. Laycock, *Thinking on its own: AI in the NHS*, Reform, 2018, 1, 17-22, https://allcatsrgrey.org.uk.

[6] F. Cabitza, D. Ciucci and R. Rasoini, *A Giant with Feet of Clay: On the Validity of the Data that Feed Machine Learning*, in *Medicine*, in F. Cabitza, C. Batini and M. Magni (eds.), *Organizing for the Digital World. Lecture Notes in Information Systems and Organisation*, Cham, Springer International Publishing, 2019, 122.

[7] Department of Health and Social Care, *The future of healthcare: our vision for digital, data and technology in health and care*, 2018, https://www.gov.uk/. This policy paper contains a range of use cases related to the applications of AI in the UK National Healthcare System.

[8] V.V. Khanna, K. Chadaga, N. Sampathila, S. Prabhu and R. Chadaga, *A machine learning and explainable artificial intelligence triage-prediction system for COVID-19*, in *Decision Analytics Journal*, vol. 7 (100246), 2023, 1, 2, https://doi.org/10.1016/j.dajour.2023.1002.46; M.A. Deif, A.A.A. Solyman, M.-H. Alsharif and P. Uthansakul, *Automated Triage System for Intensive Care Admissions during the COVID-19 Pandemic Using Hybrid XGBoost-AHP Approach*, in *Sensors (Basel)*, vol. 21, no. 19, 2021, 6379, 1-17, Doi: 10.3390/s21196379.

[9] See S. Locke, A. Bashall, S. Al-Adely, J. Moore, A. Wilson and G.B. Kitchen, *Natural language processing in medicine: A review*, in *Trends in Anaesthesia and Critical Care*, vol. 38, 2021, 4-5.

[10] H. Ronte, K. Taylor and J. Haughey, *Medtech and the Internet of Medical Things How connected medical devices are transforming health care*, Deloitte Centre for Health Solutions, 2018, 1, 2, 10, www2.deloitte.com.

[11] C.W.L. Ho, J. Ali and K. Caals, *Ensuring trustworthy use of artificial intelligence and big data analytics in health insurance*, in *Bulletin of the World Health Organisation*, vol. 98, no.4, April 2020, 264.

[12] T. Qian Sun and R. Medaglia, *Mapping the challenges of Artificial Intelligence in the public sector: Evidence from public healthcare* in *Government Information Quarterly*, vol. 36, no. 2, 2019, 368.

[13] For example, an EU-funded project, "Symptoma", developed an AI-based health chatbot that, after considering the information entered by a user, asked specific follow-up questions to identify the most likely symptoms that are strong indicators of certain diseases, assessed them, and returned a list of potential medical causes sorted by their probability. And, like many other countries, the UK developed algorithms to identify patients using datasets collected from hospital admissions, primary care EHRs and prescription records and to draw up high-risk patient lists to recommend them complete shielding. See European Commission, *Symptoma, Better Diagnosis for Patients with Rare and Complex Diseases*. CORDIS. EU results, https://cordis.europa.eu; A. Sheikh, M. Anderson, S. Albala *et al*., *Health infor-*

Not only are the NHCS engaged in the development of in-house AI applications, but also in the purchasing commercial-off-the-shelf (COTS) or bespoke software based on AI. In fact, tender notices published by contracting authorities show that European NHCS have long been procuring AI solutions for many implementations in the area of healthcare.

When considering public purchases, it is important to bear in mind that the procurement of works, services and supplies by European contracting authorities, including public entities pertaining to NHCS, is governed by Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (hereinafter, "Directive 2014/24/EU"), provided that the economic thresholds set out in Article 4 of the Directive are exceeded. In those cases, contracting authorities must procure these works, services and supplies in accordance to the procedures set forth in the Directive, and its well-established principles of freedom of access to tenders, equal treatment and non-discrimination of economic operators, transparency and proportionality of the procedures.[14]

Therefore, public procurement procedures will be the main instrument for the acquisition of AI solutions by public-health systems, being Directive 2014/24/EU a negative boundary.

3. *Are NHCS committed to procuring trustworthy AI-driven solutions?*

While the deployment and use of AI systems in the European public sector continues to escalate, there are growing concerns that specific human rights, including social rights and access to public services, are being adversely impacted by algorithmic systems.[15]

For example, discrimination-related pitfalls of AI (measurement errors, selection bias, algorithmic uncertainty, inequitable deployment or racially-tailored medicine) are common claims against the use of AI in healthcare environments.[16]

Another critical aspect is the trade-off between performance and interpretability of AI-models. Complex models may provide greater predictive capacity but less interpretable results. In this respect, the use of "black box" models in the clinical workflow would also raise concerns about the model transparency and the interpretability of the results in relation to the different stakeholders.[17]

The big question then is whether or not public procurement is keeping AI-driven solutions for the NHCS free from these adverse (individual or societal) impacts. In other words, are the NHCS buying trustworthy AI solutions? Are these solutions somehow aligned with the future European Regulation on AI?

To properly answer these questions, it is first necessary to draw a reliable map of the state of public procurement. This will enable us to analyse the extent to which tender specifications have put in place appropriate safeguards to ensure that planned purchases mitigate the inherent risks of AI.

3.1. *Constraints to a reliable mapping of AI procurement for the NHCS*

There is no clear map of AI procurement in the public sector. This opaqueness is due to several reasons.

Firstly, the instruments to ensure the publicity of tenders (aggregated tender platforms or buyers' profiles) are not designed for general transparency and public-information purposes but to provide bidders access to tenders with a view to increase equal treatment for all interested parties, efficiency and transparency of the procurement

mation technology and digital innovation for national learning health and care systems in *Health Policy*, vol. 3, July 2021, 383-396, 394-395. www.thelancet.com.

[14] See Recitals (1), (90) and Article 18(1) of the Directive 2014/24/EU.

[15] Council of Europe, *Algorithms and human rights: study on the human rights dimensions of automated data processing techniques and possible regulatory implications*, 2018, 30, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5. In particular, the Council has identified a major risk of "social sorting in medical data as algorithms can sort out specific citizen groups or human profiles, thereby possibly preventing their access to social services".

[16] S. Hoffman and A. Podgurski, *Artificial Intelligence and Discrimination in Health Care* in *Yale Journal of Health Policy, Law, and Ethics*, vol. 19 (3), 2020, 1-49, http://hdl.handle.net/20.500.13051/5964.

[17] J. Gerlings, M. Søndergaard Jensen, and A. Shollo, E*xplainable Al, But Explainable to Whom? An Exploratory Case Study of xAI* in C.P. Lim, A. Vaidya *et al*. (eds.), *Healthcare in Handbook of Artificial Intelligence in Healthcare. Vol. 2: Practicalities and Prospects*, Cham, Springer, 2022, 169, 172-174.

procedures.[18]

Secondly, the decentralisation of the instruments to ensure the publication of tender's notices and the different scope of the obligations to publish pertinent information on tenders[19] may lead not only to different levels of transparency depending on the public sector (national, regional or local), but also to a real fragmentation of the public-procurement information.[20]

Thirdly, the design of user interfaces on procurement platforms and the usability standards applied to tender portals or buyer profiles also vary among European countries and contracting authorities. This variation leads to technical gaps that impede a genuine identification of tenders of interest and access to relevant tender information. For example, the predefined search criteria of the Spanish tender platform, PLACE,[21] result in technical constraints that make it very complex to produce a complete, systematic and reliable map of public purchases of AI-enabled solutions across the NHCS.[22]

Even if the tendering platforms allow a free-text option as a search criterium, this feature does not ensure a comprehensive identification of the tenders of interest when the keywords used in the query are not present in the contract title. Turning to the French contracting system, the keyword "intelligence artificielle" (or related terms such as "machine learning", "deep learning", or similar) did not return any tenders of interest on the platform, "Plataforme des Achats de l'État",[23] although there is evidence that NHCS contracting authorities have launched calls for tenders of AI solutions.[24]

In the UK, "Find a Tender" is a service for searching and tendering for high-value contracts (over £138,760 including VAT). Unlike other European tendering platforms, Find a Tender's search tool is not restricted by the fact that the keywords used must appear in the title of the contract. For example, if one enters "artificial intelligence" + "NHS" as search criteria, the platform returns 39 notices.[25] In turn, the UK platform only provides a summary description of the specifications, whereas others in the EU usually publish all relevant documents associated with the tenders and, most interestingly, also the technical and administrative specifications.[26]

3.2. *Discussion and goals*

The future EU Regulation on AI ("AIA")[27]

[18] See Recital (52) of the Directive 2014/24/EU.

[19] See, *inter alia*, Articles 48 (prior information notices), 49 (contract notices), 50 (contract award notices), 51 (form and manner of publication of notices) or 53 (electronic availability of procurement documents) of the Directive 2014/24/EU.

[20] Cfr. J.M. Gimeno Feliú, *La reforma comunitaria en materia de contratos públicos y su incidencia en la legislación española. Una visión desde la perspectiva de la integridad*, in J.M. Gimeno Feliú, I. Gallego Córcoles, F. Fernández González and J.A. Moreno Molina (eds.), *Las Nuevas Directivas de Contratación Pública*, X Congreso de la Asociación Española de Profesores de Derecho Administrativo, Pamplona, Thomson-Reuters Aranzadi, 2015, 37-105, 50.

[21] The Spanish Public Sector Procurement Platform ("Plataforma de Contratos del Sector Público") is the online platform that enables the open consultation of tenders published in the Buyer's Profiles of the State, regional, and local contracting authorities hosted on the platform, as well as those of other public bodies utilizing different procurement platforms but publishing their calls for tender and results through aggregation mechanisms in PLACE. See Ministry of Finance and Civil Service, *Plataforma de Contratación del Sector Público*, available at https://contrataciondelestado.es.

[22] The predefined search criteria include the tender reference docket (if known), identification of the contracting authority, choice of contract type, Common Procurement Vocabulary (CPV) code, or date range. By using the pre-defined search criteria, the tool often returns a lengthy list of contracts. This poses a practical challenge in discriminating those tenders of interest for the purposes of the research. Conversely, free text cannot be used as a search criterion.

[23] See the French Platform, also called "PLACE", available at https://www.marches-publics.gouv.fr/ (last access on 28 January 2024).

[24] Assistance Publique-Hôpitaux de Paris, *L'AP-HP s'engage dans un partenariat d'innovation et va utiliser l'intelligence artificielle pour le codage des diagnostics des séjours courts*, 12 September 2019, https://www.aphp.fr/.

[25] GOV.UK, *Find a tender*, https://www.find-tender.service.gov.uk/ (last access on 28 January 2024).

[26] In the context of public purchases of AI solutions, access to tender documents is essential for a reliable mapping of AI-driven purchases in the public sector. The analysis of those documents provides very useful insights into the state-of-the-art of the solutions, thereby allowing the traceability of the specific (technical or legal) requirements in order to assess whether or not public purchases have an appropriate risk approach in relation to the intended purpose of the AI systems implemented in the NHCS.

[27] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain union legislative acts, Brussels, 21 of April 2021 (COM/2021/206 final). Although at the time of writing, EU co-legislators are still engaged in trilogue negotiations to agree on the final text after the amendments proposed by the Council and the Parliament, for the purposes of this paper, references to the AIA will be done in relation to the proposal of the European Commission, including appropriate ref-

is intended to set out horizontal obligations for high-risks AI systems, including those having adverse impacts on health, security and fundamental rights. At the same time, a growing body of soft law is emerging at the international and European level to provide standards for the implementation and development of trustworthy AI.

However, when planning the acquisition of AI-enabled solutions for the NHCS, the lack of a regulatory framework should not prevent contracting authorities from putting in place specific measures to adequately address inherent risks of AI acquisitions.

It is, therefore, necessary to assess the extent to which current public-procurement rules, procedures, and specifications ensure the implementation of trustworthy AI, aligned with the future AIA in the public sector at large, and especially within the public-healthcare systems.

Considering the above scenario, this paper seeks to:

1. Provide a general mapping of public procurement of AI solutions in the EU NHCS (identification of the procurement of innovation strategies rolled out, taxonomies of procurement procedures used, and characterisation of the AI solutions tendered);
2. Identify potential interdependencies between the risks inherent in AI and those associated with the procurement process;
3. Examine whether the tender specifications ensure that the AI solutions purchased –whether COTS or custom software– provide sufficient guarantees for reliable AI in accordance with the future AIA and emerging standards.

3.3. *Methodological approach*

To achieve the foregoing goals, multidisciplinary resources have been consulted, including but not limited to various tendering portals (eTendering, Italy, Spain), sectoral legislation applicable to public procurement and AI, soft law, guidelines for AI procurement from international organisations or European public purchasers, or works from the fields of computer sciences, biomedical research and ethics.

The scope of our review has comprised general databases (Scopus, Web of Science, ProQuest, or Dialnet); and databases specialised in health (Science Direct, Pubmed or medRxiv).

The timeline has covered from 2015 to 2023, and the languages of research were English and Spanish. The search string to identify relevant literature has included the keywords 'Artificial Intelligence' AND 'Healthcare' AND 'Public procurement'.

The analysis of the documents retrieved reveals two major findings.[28]

On the one hand, the existing research on public procurement of AI focuses mainly on general topics such as:

1. The use of AI for the innovation of procurement procedures (e.g. automatic definition of product requirements, support in negotiation and supplier selection, prediction of bidder's offers, procure-to-pay compliance, anomaly detection);[29]
2. The general identification of the associated risks to public purchasing of AI (eg. transparency, robustness and societal/individual impacts, human oversight, AI impact assessments, audits, and legal control of AI for decision making);[30]

erences to the amendments introduced by the EU Parliament and Council when necessary. The trilogue meetings between the European Commission, Council and Parliament started last June and continued in July, September, October and December 2023. See European Parliament, *Legislative Train Schedule. Artificial intelligence act. In "A Europe Fit for the Digital Age"*, 20 October 2023, https://www.europarl.europa.eu. In the last phase of the trilogue meetings, a Draft Agreement version was released on 21 January 2024. The text is available at https://artificialintelligenceact.eu.

[28] It is important to note that the purpose of this literature review is not to carry out a bibliometric study, but to identify relevant publications on public procurement of AI within the public healthcare sector.

[29] M. Guida, F. Caniato, A. Moretto and S. Ronchi, *The role of artificial intelligence in the procurement process: State of the art and research agenda*, in *Journal of Purchasing and Supply Management*, vol. 29, no. 2, 2023 (100823), https://doi.org/10.1016/j.pursup.2023.100823; R. Nai, E. Sulis and R. Meo, *Public Procurement Fraud Detection and Artificial Intelligence Techniques: a Literature Review* in *EKAW'22: Companion Proceedings of the 23rd International Conference on Knowledge Engineering and Knowledge Management*, Bozen-Bolzano, September 26–29, 2022, https://ceur-ws.org; S. Jiménez, A. Ortiz and D. Alonso, *Predicción de ofertas para contratos públicos. Aplicación de la inteligencia artificial a los datos de contratación*, in J.M. Gimeno Feliú (dir.), *Observatorio de los Contratos Públicos 2021*, Pamplona, Aranzadi 2022, 491-505.

[30] World Economic Forum, *Unlocking Public Sector AI. AI Procurement in a Box: Workbook. Toolkit*, June 2020 ("WEF Guidelines"), https://www3.weforum.org; J. Miranzo Díaz, *Inteligencia artificial y contratación pública*, in I. Martín Delgado and J.A. Moreno Molina (dirs.), *Administración electrónica, transparencia y con-*

3. The key aspects in the design of the procurement procedures and relevant clauses in public contracts for AI solutions,[31] or the potential inconsistencies in the contract-classification system concerning the acquisitions of off-the-shelf/ bespoke software (supply or service contracts) and management of intellectual property rights.[32]

On the other hand, out of all the literature reviewed, only a few publications specifically discuss AI procurement in the healthcare sector.[33]

To draw a first picture of the AI procurement for healthcare, general guidance on innovation procurement –be it public procurement of innovative solutions ("PPI") or pre-commercial procurement ("PCP")– has been consulted. In addition, the production of international and European standards for trustworthy IA[34] and the ongoing discussion of the future AIA have resulted in the first specific guidelines for AI procurement (World Economic Forum,[35] European Commission,[36] UK Government,[37] City of Amsterdam,[38] City of Barcelona[39]), including AI procurement in healthcare sector (UK Government[40]). Consequently, to further enrich our analysis this emerging corpus of guidance has also been considered.

This theoretical background has been completed with the creation of a database with tenders of interest. The database is part of the research project PID2021-128621NB-100 referred to above. It covers the period dating from 2015 to the present and is updated from time to time. The consultation of PLACE, other platforms and buyer profiles has resulted in the identification of nearly 60 tenders.[41] From these listed tenders, a sample has been extracted and is now presented in Annex I (Refs. [1]-[5]) and Annex II below (Refs. [6]-[20]) for the purposes of our review. Each tender is identified in the Annexes by its docket reference, and numbered from [1] to [20].

While most of the tenders are focused on the Spanish NHCS (Annex II), some tenders launched by EU institutions and retrieved

tratación pública, Madrid, Iustel, 2020, 105-142; M. Hickok, *Public procurement of artificial intelligence systems: new risks and future proofing* in *AI & Society*, October 2022, https://doi.org/10.1007/s00146-022-01572-2; E. Gamero Casado, *Supervisión, auditoría y control jurídico en la contratación pública de soluciones de robotización e inteligencia artificial para soporte a la toma de decisiones* in *Observatorio de la Contratación Pública*, October-November 2022, www.obcp.es.

[31] I. Gallego Córcoles, *La contratación de soluciones de inteligencia artificial*, in E. Gamero Casado and F.L. Pérez (coords.), *Inteligencia artificial y sector público. Retos, límites y medios*, Valencia, Tirant lo Blanch, 2023, 504-564.

[32] J. Miranzo Díaz, *La contratación pública como elemento de control, garantía e impulso de la IA pública*, 2024, https://congresoaepdavigo2024.es.

[33] See A. García-Altés A, M. McKee, L. Siciliani *et al*., *Understanding public procurement within the health sector: a priority in a post-COVID-19 world*, in *Health Economics, Policy and Law*, vol. 18, no. 2, 2023, 172–185, Doi:10.1017/S1744133122000184; L. Silsand, G-H. Severinsen, L. Linstad and G. Ellingsen, *Procurement of artificial intelligence for radiology practice,* in *Procedia Computer Science*, vol. 219, 2023, 1388-1395; K. Selviaridis, A. Hughes and M. Spring, *Facilitating public procurement of innovation in the UK defence and health sectors: Innovation intermediaries as institutional entrepreneurs*, in *Research Policy*, vol. 52, no. 2, 2023, https://doi.org/10.1016/j.respol.2022.104673.

[34] OECD, *Recommendation of the Council on Artificial Intelligence* of 22 May 2019 ("OCED Recommendations"); High-Level Expert Group on Artificial Intelligence, *Ethics guidelines for trustworthy AI,* European Commission, 8 April 2019 ("HLEG Ethics Guidelines").

[35] WEF Guidelines, 1-17.

[36] European Commission, Proposal for standard contractual clauses for the procurement of Artificial Intelligence (AI) by public organisations. High-Risk version, September 2023 ("European Commission H-R Standard Clauses") https://public-buyerscommunity.ec.europa.eu. Although, for the purposes of this paper, the reference to the European Commission's standard clauses will, in most cases, be made to this high-risk version, there is also a non-high-risk version, applicable to other algorithmic systems that does not necessarily qualify as 'AI systems.' This latter version seeks to cover simpler software rule-based systems, given that their use in the public sector may also require increased accountability, control and transparency in certain cases.

[37] Office for Artificial Intelligence, *Guidelines for AI procurement. A summary of best practice addressing specific challenges of acquiring Artificial Intelligence technologies in government*, 8 June 2020 ("UK Guidelines"), https://www.gov.uk/.

[38] City of Amsterdam, *Standard Clauses for Procurement of Trustworthy Algorithmic Systems*, version 2.0, 17 June 2021, ("Amsterdam Standard Clauses"), https://www.amsterdam.nl.

[39] City of Barcelona, *Definition of work methodologies and protocols for implementing algorithmic systems*, 31 January 2023 ("Barcelona Methodologies"), https://ajuntament.barcelona.cat.

[40] J. Joshi and D. Cushnan, *A buyer's guide to AI in health and care. 10 questions for making well-informed procurement decisions about products that use AI*, NHS England Transformation Directorate, 2020 ("UK NHS Buyer's Guide"), https://transform.england.nhs.uk.

[41] Systematizing the selected tenders and analysing their respective tender documents, including preliminary market consultations, and memoranda justifying the public need addressed by the contract, have allowed the development of this database leading to the initial analysis of the state of public procurement for AI solutions within the NHCS.

from the eProcurement platform, "TED. eTendering", have been also considered (Refs. [1]-[3]).[42] To complete our sample, some tenders of the Italian Agenzia Nazionale per i Servizi Sanitari Regionali ("AGENAS")[43] have been listed as well.

Consultations through the national procurement platform in Spain, PLACE, have identified some contracts dating back to 2015 and 2016 (Ref. [6], [7] in Annex II).

To illustrate the current state of AI-solution procurement for the NHCS, constant references are made to the 20 tenders in the sample. Additionally, insights are extracted from tender specifications across 21 tables.

The analysis of tender specifications has been conducted based on two criteria: (i) identification and characterisation of the public-procurement procedures applied, and (ii) characterisation of AI-solutions in healthcare. The first criterion offers insights into the challenges associated with the procurement process, while the second one provides a view of what the NHCS is procuring and allows us to identify potential risks inherent in the disruptive nature of AI technology.

The application of the criteria above results in the identification of the following risks in the public procurement of AI solutions for the NHCS.

Risks inherent in procurement procedures	**Risks inherent in AI solutions**
- Potential inconsistencies arising from the interaction with harmonized legislation (eg. AIA or Medical Devices Regulations); - Lack of national or regional strategies for AI; - Lack of planification of AI purchases; - Complexity and length of the procedure; - Lack of multidisciplinary teams and skills; - Inadequate identification of public needs to be met; - Management of Intellectual Property rights and vendor lock-in effects	- Regulatory compliance of legacy AI systems; - Lack of prior AI impact assessment - Determining whether or not AI is the right solution; - Purchasing COTS software vs bespoke software; - 'Gold-plated' *versus* 'functional' specifications; - The intended purpose and the evolving nature of AI systems; - Lack of provisions in tender specifications ensuring trustworthy AI/future alignment with AIA (eg. data quality, transparency and explainability, performance and error metrics).

Table 1. Inherent risks in AI procurement

4. *What is being procured by the NHCS? The challenging interaction between the future AIA and MDR/IVRDR Regulations*

A thorough literature review shows that the transformative potential of AI for healthcare includes a bundle of applications in the following major areas:[44]

1. AI in clinical practice: clinical-decision support with alerts and reminders, prognosis and risk prediction, medical image interpretation (contouring, segmentation and pathology detection), emergency medicine, surgery, adaptative interventions, tools integrated with EHR;
2. AI solutions for patients and their families: personalised treatments, conversational agents, telemedicine and health monitoring, timely personalized intervention, assistance for individuals with disabilities;
3. AI in healthcare administration: patient-flow management, coding, scheduling, detection of fraudulent activity, healthcare audits;
4. AI in biomedical research: clinical research, drug discovery, clinical trials, mining EHR data and extraction of patterns, phenotyping, improved access to

[42] European Commission, *TED.eTendering* in *SIMAP. Information system for public procurement*, https://etendering.ted.europa.eu/. Notice that TED eTendering will be gradually discontinued and replaced by the Funding and Tenders (F&T) Portal.

[43] AGENAS, *Gare in corso*, www.agenas.gov.it/bandi-di-gara-e-contratti/avvisi-bandi-e-inviti/gare-in-corso.

[44] K. Lekadir, G. Quaglio, A. Tselioudis Garmendia and C. Gallin, *Artificial intelligence in healthcare. Applications, risks, and ethical and societal impacts,* European Parliamentary Research Service (EPRS), Panel for the Future of Science and Technology (STOA), 2022, 5-14, Doi:10.2861/568473; M. Matheny, S. Thadaney Israni, M. Ahmed and D. Whicher (Ed.) *Artificial Intelligence in Health Care. The hope, the Hype, the Promise, the Peril*, Washington DC., National Academy of Medicine, 2022, 65-86. See also, E. Harwich and K. Laycock, *Thinking on its own: AI in the NHS*, January 2018, 17-22, https://allcatsrgrey.org.uk; G. Mahadevaiah, P. RV, I. Bermejo *et al.*, *Artificial intelligence-based clinical decision support in modern medical physics: Selection, acceptance, commissioning, and quality assurance* in *Medical Physics*, vol. 47, issue 5, 2020, e228-e235, e229, https://doi.org/10.1002/mp.13562.

biomedical literature;
5. AI for public health: health communication and AI-enabled health campaigns, chronic-disease management, disease surveillance, environmental and occupational health, prior authorisation in healthcare benefits and pharmacy.

Most of the AI solutions in the sample of Annex I and II can be included in one or more of the applications above.

Areas of application	Tenders of interest
Pathology detection, clinical decision support, personalised medicine.	[16][17] [18]
Delivery of remote-healthcare services (telemedicine, telerehabilitation, personal assistants, self-care).	[5] [10] [20]
Management and optimisation of available healthcare resources (patient triage, waiting lists, effectiveness of treatments).	[8] [13]
Secondary uses of health data (analysis of data for biomedical research).	[16] [17]
Research and development, consultancy services on AI applications in healthcare.	[1] [7]
Promotion and improvement of health services (e.g. sentiment analysis and assessment of health services by end-users, promotion of healthy lifestyles).	[4] [6] [18]
Epidemiological predictive analysis and early-warning of public-health threats.	[2] [3]
Fraud detection in social benefits.	[12]
Provision of data repositories (e.g. Health Data Lakes) and IT infrastructures supporting AI models based on cloud (PAAS, SAAS, IaC) or on premise.	[4] [5] [13] [14] [15] [16] [19] [20]

Table 2. Application of AI in the NHCS

4.1. *Purchasing AI-solutions for NHCS likely under the future AIA*

Following Article 3(1) of the AIA, an AI system is a "software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with". For example, many of the tenders in the sample include use cases aimed at developing AI models to make predictions or recommendations.

Output model	Description in tender specifications
Predictions	Predicting the number of emergency admissions in relation to airborne particle concentration [18]. Prediction of weaning failure and length of stay in ICU [19].
Recommendations	Recommendation engine that suggests which patients on the waiting list should be prioritised for surgery based on their personal, clinical, social and urgency characteristics to potentially reduce waiting times [13].

Table 3. Output models in tender specifications

Considering the definition of the "AI systems" proposed by the European Commission, many of the sampled contracts imply the development of one or more techniques and approaches listed in Annex I of the AIA, in particular, ML approaches (including supervised, unsupervised, reinforcement learning, DL); logic and knowledge-based approaches (including knowledge bases, inference and deductive engines or expert systems) or statistical approaches, Bayesian estimation or search and optimisation methods.[45]

[45] However, the list of techniques proposed by the Commission has been discussed by the EU institutions. The Economic and Social Committee found no added value in Annex I and recommended removing it entirely from the AIA, as some of the techniques are not considered AI by AI scientists and a number of important AI techniques would be missing in the Commission's Proposal (see EESC 2021/02482, of 22 December of 2021, par. 3.2). According to the Parliament mandate, the definition of AI systems should be amended to align with the definition agreed by the Organisation for Economic Co-operation and Development (OECD) and suppress Annex I, while the Council narrowed down the definition to systems developed through ML approaches and logic- and knowledge-based approaches and supressed Annex I (see ST 15698 2022 INIT, 15698/22, of 6 December 2022). At the time of writing and at this point of the trilogue negotiations, it appears that the Commission, Parliament and Council have not reached an agreement on Annex I. However, the co-legislators have proposed a new definition of "AI systems" catching the adaptative nature (*continuous learning*) of AI systems (which is typical of many ML models). The common definition proposed reads as follows: "An AI system'

Looking at the tender specifications of the AI solutions in the sample, some of them describe the application of AI in a very broad way, without detailing or prescribing a concrete AI technique or approach (Refs. [1], [10], [11], [15]), whereas other tender documents indicate the specific learning approaches to be implemented, such as ML and DL (Refs. [2]-[5], [7], [9], [13], [14], [16], [18-20]), including expert systems (Refs. [7], [8]), or statistical learning (Ref. [16]). Some tender specifications define in a very detailed way the learning problem to be addressed by the contractor, e.g. regression, classification, clustering, anomaly detection, or structured prediction.[46]

Learning problem	Description in tender specifications
Regression	- Predicting the duration of sickness absence due to illness or accident [12]. - Prediction of unscheduled readmissions in the month following discharge [18].
Classification	- Selection of patients for active search in rare diseases [13]. - Comparison of the results of pharmacological treatments (success or failure cases), based on the different prescriptions made for pathologies of the same nature [13].
Clustering	- Group population to benefit from primary and secondary prevention [4]. - Grouping chronic patients based on similarities to personalise healthcare and optimise the use of resources based on the level of care prescribed by the healthcare professional [18].
Anomaly detection	- Monitoring Telemedicine platform with advanced analytics systems capable of detecting anomalous patterns that are not obvious or even new, using ML [4].
Dimensionality reduction	- Disease prevention and control and early warning of public-health threats using social media by applying unsupervised ML/DL models on dimensionality reduction for data compression [3].
Structured prediction	- Segmentation of mammography and pathological-anatomy imaging to predict the cancer-risk index in a marked area of the image, and to produce marks on the processed images to identify the detection made [11].

Table 4. Learning problem in tender specifications

4.2. *Qualification of an AI system as a Medical Device Software (MDSW)*

Most of the tenders of interest include the design, development and deployment of AI-driven software and applications with an intended medical purpose.

In principle, the fact of being AI-based software tools and, at the same time, software to be used for an intended medical purpose, either on its own right, or driving or influencing the use of a (hardware) medical device or *in vitro* diagnostic medical device, would trigger the application of the AIA and Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices ("MDR") or Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on *in vitro* diagnostic medical devices ("IVMDR")[47] (hereinafter jointly, "MD Regulations"). As explained below some of the AI solutions listed in Annexes I and II could qualify as MDSW under the MD Regulations.[48]

AI-driven software[49] to be used, alone or in

(AI system) is a machine-based system designed to operate with varying levels of autonomy and that *may exhibit adaptiveness after deployment* and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (see Draft Agreement of 21 January 2024).

[46] In relation to tasks and learning problems in ML, see ISO/IEC 23053:2022(en) Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML), at 5-7.

[47] Cfr. K. Lekadir *et al*., *Artificial intelligence in healthcare*, 31; F. Zanca, C. Brusasco, F. Pesapane *et al*., *Regulatory Aspects of the Use of Artificial Intelligence Medical Software*, in *Seminars in Radiation Oncology*, vol. 32, no. 4, 2022, 432-433, https://pubmed.ncbi.nlm.nih.gov.

[48] It should be noticed that MD Regulations entered into force on 16 March 2022, and many provisions were scheduled to take effect gradually.

[49] For the purposes of this paper, the term "software" is aligned with the definition given by Medical Device

combination, for one or more of the *specific medical purposes* laid down by the MDR[50] could qualify, in principle, as medical-device software (MDSW). This includes software modules (eg. module providing and expert-system assistance for medical-decision making) and applications (e.g. operating on a mobile phone, in the cloud or on other platforms) with a medical purpose.[51]

Typical examples of medical devices qualified as MDSW would be decision-support software which "combine general medical information databases and algorithms with patient-specific data" (e.g., Ref. [13]); telemedicine systems to "allow monitoring and/or delivery of healthcare to patients at locations remote from where the healthcare professional is located" (e.g., Ref. [5]); telesurgery "to conduct a surgical procedure from a remote location" (using, for instance, virtual reality); or web systems "for the monitoring of clinical data" which "interacts with a medical device (e.g. implanted devices or homecare devices), and uses a transmitter to send the information over the internet or a mobile network"[52] (e.g., Ref. [20]).

In particular, decision-support software would usually be considered a medical device when it applies automated reasoning, such as algorithms or more complex series of calculations, provided that: (i) it is linked to a specific medical device, or (ii) it is intended to influence the actual treatment (e.g., dose, time of treatment), or (iii) it results in a diagnosis or prognosis (e.g., providing future risk of disease).[53]

In the same vein, AI-driven software intended to be used, solely or principally, for the purpose of providing information on one or more of the functions listed under IVMDR could qualify as *in vitro* diagnostic medical device.[54] This would be the case of an AI tool that assists or replaces clinicians in the examination of prepared biopsy samples,[55] an Image Management System (IMS) which incorporates complex quantitative functions to support post-processing of images for diagnostics purposes[56] (e.g., Ref. [11], [13][57]),

Coordination Group ("MDCG") established by the Article 103 of the MDR. The MDCG defines "software" as "a set of instructions that processes input data and creates output data". In particular, AI-driven software computes input data (e.g. data given through speech recognition, formatted for medical purpose records such as DICOM file or ECG or EHR, data received from/transmitted by devices or unformatted clinical documents in paper) to produce output data (e.g. audio data, digital or printed documents, screen display data –including numbers, characters, picture, graphics) in the form of content, predictions, recommendations, or decisions. Cfr. MDCG, *Guidance on Qualification and Classification of Software in Regulation (EU) 2017/745 – MDR and Regulation (EU) 2017/746 – IVDR*, October 2019, 5, https://health.ec.europa.eu.

[50] Article 2(1) of the MDR define 'medical device' as "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination, for human beings for one or more of the following specific medical purposes:
- diagnosis, prevention, monitoring, prediction, prognosis, treatment or alleviation of disease,
- diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability,
- investigation, replacement or modification of the anatomy or of a physiological or pathological process or state,
- providing information by means of in vitro examination of specimens derived from the human body, including organ, blood and tissue donations,
- and which does not achieve its principal intended action by pharmacological, immunological or metabolic means, in or on the human body, but which may be assisted in its function by such mean".

[51] MDCG, *Guidance*, 3, 17-18.

[52] *Idem*, 18-23. By contrast, software intended for non-medical purposes, such as invoicing or staff planning or software for general purposes supporting communication systems to transfer electronic information (e.g., prescription, referrals, images, patient records), do not qualify as medical-device software.

[53] Cfr. Medicine & Healthcare Products Regulatory Agency (UK), *Guidance: Medical device stand-alone software including apps (including IVDMDs)*, 12, www.gov.uk/.

[54] MDSW fulfilling the definition of an *in vitro* diagnostic medical device falls under Article 2(2) of the IVMDR, provided that it is intended to be used "solely or principally for the purpose of providing information on one or more of the following: (a) concerning a physiological or pathological process or state; (b) concerning congenital physical or mental impairments; (c) concerning the predisposition to a medical condition or a disease; (d) to determine the safety and compatibility with potential recipients; (e) to predict treatment response or reactions; (f) to define or monitoring therapeutic measures."

[55] Cfr. Medicine & Healthcare Products Regulatory Agency, *Guidance: Medical device*, 13.

[56] MDCG, *Guidance*, 23.

[57] Pursuant to Article 48 of the IVMDR Devices in Classes B, C and D do require a conformity assessment by a notified body. In addition, Rule 3 stipulates that *in vitro* devices are classified as class C if they are intended, *inter alia*, to be used in screening, diagnosis, or staging of cancer. For example, among the use cases listed in the technical specifications related to the advanced analytics for the Public Health System of Andalusia launched Red.es (Ref. [13]), the 'radiological imaging analysis to support breast cancer screening' is aimed at generating a pre-diagnosis in mammography images for breast cancer screening. This imaging analysis using AI would help identify which images should be studied by radiodiagnostic specialists with the highest priority. According to the specifications, the scope of the case

or expert systems intended to provide information for predicting predisposition to any specific disease by capturing and analysing multiple results obtained for one patient by means of *in vitro* examination of body samples, possibly combined with information from medical and non-medical devices[58] (e.g., Ref. [17]).

Where the intended purpose of the MDSW output data falls under both the definitions set out in the MDR and IVDR, a weighting of the data sources based on how determinant the information is to fulfil the intended medical purpose should be conducted to determine which Regulation applies to the MDSW.[59]

It is clear, then, that MDR and IVMDR apply to medical devices and *in vitro* MDSW, including AI-driven software. The examination of the tenders in the sample shows that certain contracts are classified as supply of medical-software packages (Ref. [20]) or medical-software development services [Ref. [5], [17], [20]).

Qualifying an AI system as a medical device triggers the application of number of obligations provided by the MD Regulations,[60] among others, the third-party conformity assessment and the CE marking. Some of the tenders in the sample, including the development of medical software based on AI, require the provision of mandatory CE marking of conformity (Refs. [5], [13], [20]).[61]

However, despite the long list of quality and safety requirements, many aspects specific to AI that may adversely impact on health are not addressed by the MD Regulations (e.g., continuous learning of the AI models, identification of algorithmic biases, transparency and explainability of complex models, trade-offs between performance and accuracy).[62]

4.3. *To be or not be a 'high-risk system': constraints associated with the in-house exception*

According to the risk approach followed by the AIA (unacceptable risk, high risk, limited risk, and low or minimal risk), AI systems identified as 'high-risk' are identified with those having a "significant harmful impact on the *health*, safety and fundamental rights of persons in the Union [emphasis added]". In particular, "in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate". Consistently, those risks generated by AI systems should be "duly prevented and mitigated".[63]

Considering the wording of the AIA, it appears that the EU legislator implies that AI

would end in the satisfactory statistical validation, "excluding any *potential requirements for homologation and CE marking necessary* for the systematic use of the tool in the healthcare field [emphasis added]". See Red.es, *Pliego de Prescripciones Técnicas que regirán la realización del contrato de "servicio para la implantación de una solución corporativa de analítica avanzada, basada en tecnologías Big Data, para el sistema sanitario público de Andalucía"*, 18 January 2021, 89, https://contrataciondelestado.es/.

[58] MDCG, *Guidance*, 22.

[59] *Idem*, 10-11, 24. For example, a given MDSW is designed to reduce ICU transfers, readmissions, adverse events and length of stay by generating a risk score to trigger care processes. By default, the risk score includes respiratory rate, heart rate, blood pressure and peripheral oxygen saturation (SpO2). However, a user can configure it to include other parameters, including results from *in vitro* diagnostic medical devices. The intended purpose of the device includes "concerning a physiological or pathological process or state (by investigation of this process or state)" (Article 2(2)(a) of the IVMDR); "to define or monitoring therapeutic measures" (Article 2(2)(f) of the IVMDR); "diagnosis, monitoring, treatment, alleviation of, or compensation for, an injury or disability" (Article 2(2) (h) of the MDR). In principle, the information provided by the MDSW and the intended purpose of the software are within the scope of the in vitro diagnostic medical device definition. Yet, the significance of the information derived from the medical device drives the intended purpose. This is because the data received from the *in vitro* diagnostic medical device are not considered to be determinative for the overall calculation result (output) achieved by the MDSW, resulting in the qualification of the software as an MD MDSW subject to the MDR.

[60] Among others, a stricter pre-market control, increased clinical investigation requirements, third-party conformity assessment with a view to the placing on the market or putting into service, reinforced and continuous monitoring across the device's lifecycle, and improved transparency.

[61] For example, in the ROSIA project (Ref. [20]), it was expected that some of the proposed solutions would fall within the scope of the MDR. Therefore, bidders were requested to describe, in their technical proposals, whether any of the elements had already been approved for conformity declaration. If not, they were asked to specify the stage at which they were in the process of obtaining approval. See Instituto Aragonés de Ciencias de la Salud, *ROSIA. Tender Forms Call for Tender Phase 2. Technical Specifications,* Docket No. PHASE 2 ROSIA PCP 101017606, 1 February 2023, 13, https://contrataciondelestado.es/.

[62] Cfr. K. Lekadir *et al*., *Artificial intelligence in healthcare*, 30.

[63] Recitals (27) and (28) of the AIA. Both the Council and the Parliament's versions retain the same wording as the AIA on this point.

systems deployed and used in healthcare are likely to be qualified as inherently 'high-risk systems.' Simply put, many AI tools that qualify as MDSW under the MD Regulations would also be considered 'high-risk systems' pursuant to the AIA.[64] This interpretation is supported by some scholars.[65]

However, a careful examination of the interplay between the MD Regulations and the AIA shows that some MDSW, in principle qualified as medical devices or *in vitro* diagnostic medical devices, would fall out of the scope of Article 6 of the AIA.

While a case-by-case analysis would be necessary, pursuant to Article 6 of the AIA, high-risk systems would comprise:
(i) AI systems qualified as MDSW under the MD Regulations, provided that they are subject to a third-party *ex-ante* conformity assessment[66] –Article 6(1)(a) and (b);
(ii) Certain stand-alone AI systems listed in Annex III of the AIA, in particular, those AI systems which evaluate or condition access to and enjoyment of public services and benefits[67] – Article 6(2).

Both "high-risk" classification rules in Article 6 of the AIA call for further clarification to determine the applicability of the horizontal requirements (Articles 9-15) and obligations (Articles 16-29) laid down in the AIA.[68]

From a public-procurement perspective, the criterion of an *ex-ante* third-party conformity assessment under the MD Regulations would significantly reduce the number of AI-driven MDSW that would qualify as 'high-risk' systems, regardless of their adverse impact on health.

Essentially, by exempting MDSW from the *ex-ante* conformity-assessment obligation, the application of the 'in-house exemption' implies removing one of the *concurring conditions* laid down in Article 6(1)(b) of the AIA to qualify an AI system as 'high-risk'. Consequently, if one of the substantive conditions is not met, then the medical device would not qualify as a 'high-risk' system.

The in-house exemption applies to medical devices that are manufactured and used within the same EU health institution[69] on a non-industrial scale to address specific needs of target-patient groups which cannot be met at the appropriate level of performance by an equivalent CE-marked device available on the market.[70]

Except for the relevant general-safety and performance requirements specified in Annex I of the MDR and the IVDR, in-house medical devices are exempt from most provisions of the Regulations, including conformity-assessment procedures.[71] Article 5(5) of both

[64] Cfr. K. Lekadir *et al*., *Artificial intelligence in healthcare*, 31, finding that "[i]t appears that many medical AI tools, especially those that are autonomous, will be categorised as high-risk."

[65] See H. Van Kolfschooten, *EU regulation of artificial intelligence: challenges for patients' rights*, in *Common Mark. Law Rev*. 59(1), 81–112 (2022), http://dx.doi.org/10.2139/ssrn.3997366. The author found that "'[h]igh risk' includes AI-systems that are intended to be used in products regulated at the EU level as listed in Annex II, including the MDR. This means that all medical devices that fall under the MDR are classified as 'high risk' under the AIA."

[66] Recitals (30) and (31) of the AIA.

[67] See, in particular, Annex III (5) (a) and (c) of the AIA.

[68] On the one hand, Articles 9-15 of the AIA set forth a list of requirements in relation to quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, human oversight, and robustness, accuracy and cybersecurity. On the other hand, Article 24 would apply to product manufacturers of medical devices imposing on them the obligations set out in Articles 16-23 (putting in place a quality management system; drawing-up the technical documentation; recording of automatically generated logs; undergoing the relevant conformity assessment procedure; taking corrective actions where necessary; registration of the high-risk AI system in the EU database; duty of information and cooperation with the national competent authority; affixing CE marking), while Article 29 lists the obligations applicable to users of high-risk AI systems (use of the AI system in accordance with the accompanying instructions of use, implementation of the human oversight measures indicated by the provider, ensuring the relevance of the input data in relation to the intended purpose, monitoring the operation of the system, keeping the logs automatically generated, use of the information resulting from the transparency obligation laid down in Article 13 to conduct data protection impact assessment under the GDPR or the Directive 680/2016).

[69] A "health institution" is an organisation the primary purpose of which is the care or treatment of patients or the promotion of public health. Health institutions include hospitals, as well as laboratories and public health institutes that support the health-care system and/or address patient needs, but which do not treat or care for patients directly. The concept does not cover establishments primarily claiming to pursue health interests or healthy lifestyles (gyms, spas, wellness and fitness centers). See Recitals (30) and (29), and Articles 2(36) and 2(29) and 36 of the MDR and IVMDR, respectively.

[70] Recitals (30) of the MDR and 29 of the IVMDR.

[71] Some of the mandatory requirements laid down by the MDR and IVMDR for placing on the market or putting into service MDSW qualified as medical device or *in vitro* diagnostic medical device comprise, transparency and traceability obligations, classification of devices, conformity assessment procedures and CE marking, clinical investigations and clinical evaluation, vigilance

MD Regulations establishes the conditions to which health institutions must adhere to in order to apply this exception.[72]

Outside the scope of Article 5.5 of the MD Regulations are medical-device applications that allow patients to use the application outside the health institution. For example, patients may enter or access medical data that are subsequently used by healthcare professionals.[73] This could be the case of applications used in telemedicine, telemonitoring or telerehabilitation of patients. In this respect, some telemedicine platforms (e.g., Refs. [5], [20]) require the CE marking of conformity.

However, it is unclear whether the concept of "in-house devices" refers only to medical devices manufactured by the health institution on its own right, or includes also medical devices whose manufacture has been outsourced to a supplier through public-procurement procedures.[74]

The procurement practices of the National Health Service (NHS) in the United Kingdom may provide some insight into this particular issue. According to the NHS Guidelines, when AI-driven MDSW to be procured by the NHS consists of a COTS solution, then it will meet the two conditions (component or system covered by relevant Union-harmonisation legislation and mandatory undergo of a third-party conformity assessment) to be qualified as a 'high-risk system.' In contrast, if the AI-driven MDSW is a bespoke solution, then it will apply the *in-house* exception and, no conformity assessment will be required.[75]

In addition, Article 5(5) of the MD Regulations allows Member States to restrict the manufacture and the use of any specific type of such devices, some national legislations have constrained the scope of the in-house exception. Accordingly, in Spain, Article 9 of the Royal Decree 192/2023, of 21 March, governing medical devices, establishes that manufacture of devices by healthcare institutions for the exclusive use of the institution itself may only be carried out by healthcare institutions legally qualified as hospitals. In addition to this exclusion of healthcare institutions other than hospitals, the Spanish regulation prohibits the "subcontracting" of any of the manufacturing activities of medical devices and excludes Class IIb, Class III and implantable devices from the scope of Article 5.5 of the MDR.

Together with AI medical software subject to the MD Regulations, the AI systems described in Annex III of the AIA are qualified as 'high risk' systems. These stand-alone systems may include specific applications in health, in particular, AI systems intended to be used by public authorities or on behalf of public authorities in the area of healthcare to evaluate the eligibility of natural persons for public-assistance benefits and services, as well as to grant, reduce, revoke, or reclaim such benefits and services, or to dispatch, or to prioritise the dispatching of emergency first-response services, including medical aid.[76] The

and market surveillance, continuous documentation and update of risk and quality management systems. Conformity assessment procedures are regulated in Articles 52-60 of the MDR and 48-55 of the IVMDR.

[72] The obligations under Article 5(5) of the MD Regulations include the prohibition to transfer the in-house medical device to another legal entity and industrial scale manufacturing, justification that the specific needs of a target patient group cannot be met (with the appropriate level of performance) by an equivalent device available on the market of CE-marked devices, appropriate documentation relating to the design and manufacture of the device at the disposal of a competent authority, public declaration that the applicable general safety and performance. requirements are met, implementation of an appropriate quality management system (QMS), and follow-up and reporting of incidents and corrective actions.

[73] MDCG, *Guidance*, 7.

[74] Idem, 5-6, define how the term 'manufactured' is to be understood, but does not clarify whether the manufacture must be carried out exclusively by the health institution with its own human and material resources, or whether the term 'manufactured' can also include a supplier on behalf of the health care institution using the legal instruments provided by national legislation (e.g. public procurement, administrative agreements, public-private partnerships).

[75] Cfr. NHS, *A buyer's guide*, 20, 24. The NHS guidance is aimed at the public procurement of 'off-the-shelf' AI applications, i.e. products packaged by suppliers as ready to use, which are required to meet CE marking requirements *ex ante*. The guidance clearly excludes bespoke projects, which may include *in-house* manufactured devices outside of the MD regulations.

[76] The amendment of the European Parliament to the provisions contained in Annex III (a) and (c) clarifies the scope of application to healthcare field. According to the Parliament, Annex III (a) of the AIA should read as follows: "(a) AI systems intended to be used by or on behalf of public authorities to evaluate the eligibility of natural persons for public assistance benefits and services, *including healthcare services* and essential services [emphasis added]. In addition, Annex III (c) should say: "(c) AI systems intended to evaluate and classify emergency calls by natural persons or to be used to dispatch, or to establish priority in, the dispatching of emergency first response services, including by police and law enforcement, firefighters and medical aid, as well as of *emergency healthcare patient triage systems* [emphasis added]."

amendments of the Parliament to these provisions explicitly include those AI-systems to evaluate the eligibility of natural persons for "healthcare services" and "emergency healthcare patient triage systems".

This would be the case of the expert system procured by the Regional Government of Valencia which classifies according to the risk severity of the incident the healthcare demand for emergencies, out-of-hospital emergencies and medical calls to emergency number 112 using ML/DL techniques (Ref. [8]), or the AI-based decision-support system acquired by EGARSAT, an auxiliary entity of the Social Security, for predicting the duration of sickness absence due to illness or accident which could affect social security benefits or even trigger administrative sanctions if fraudulent patterns are detected (Ref. [12]).

Even if AI systems acquired for the NHCS qualify as high-risk systems falling under the conditions of Article 6 (qualification as medical device subject to a third-party conformity assessment pursuant to the MD Regulations or stand-alone systems listed in Annex III), there would still be many other AI applications posing risks to life and health that could otherwise fall outside such a qualification. This classification means that AI-systems in healthcare that do not fall under Article 6 are formally considered to "pose 'limited risk' and therefore [are] minimally regulated under the AIA", although they may still have adverse effects on human health.[77]

This is exemplified by personal-assistant systems, like the advanced system called AVATAR procured by the Regional Health Service of Galizia (Ref. [10]),[78] which generates alerts for both patients and health professionals based on risk patterns identified by AI systems. False alerts or a lack of alert/response resulting from erroneous interpretation of risk patterns by the AI system could have adverse consequences for patients.

However, exemptions –as those illustrated above– from the stricter regime provided by the AIA for high-risk systems would clearly contradict the wording of Recital (28) of the Proposal.[79]

5. *AI solutions for NHCS in the context of innovation procurement*

While digitisation and digitalisation[80] are prerequisites for AI applications, this data-driven technology is a further step in digital transformation. AI is reshaping organisations and augmenting organizational innovation[81] through the introduction and implementation of new or significantly-improved goods, services, methods or organisational practices.

In particular, AI involves a "transformational potential" for healthcare services, by "supporting diagnostic decisions, predicting care needs, informing resource planning, and game-changing research".[82]

[77] See Van Kolfschooten, *supra* cited.

[78] According to the technical specifications, the advanced personal assistant includes:
User interfaces enabling patients to receive information adequately from health professionals and the health system.
A module that integrates automated devices for collecting events related to physiological parameters, movement, displacement, or behavior of patients within the autistic spectrum, those with visual or hearing difficulties, or neurodegenerative diseases. The most relevant variables identified for triggering immediate alerts and/or actions include heart rate, arrhythmias or cardiac arrest, sleep rhythm, loss of consciousness, convulsive crises, and time-distance control (geolocation of the patient and monitoring distance from specific points like home or residence).
Advanced functionalities utilizing AI techniques, along with facial, postural, and voice recognition systems for detecting physiological and/or behavioral patterns. These patterns can be correlated with event information and existing data in health center information systems, such as medical records.
A module capable of generating alerts and individualized warnings for patients, caregivers, and professionals based on identified patterns associated with high-risk situations.

[79] In relation to the classification of an AI system as high risk, Recital (28) of the AIA says: "AI systems could produce adverse outcomes to health and safety of persons, in particular when such systems operate as components of products […] Similarly, *in the health sector where the stakes for life and health are particularly high, increasingly sophisticated diagnostics systems and systems supporting human decisions should be reliable and accurate*. The extent of the adverse impact caused by the AI system on the fundamental rights protected by the Charter is of particular relevance when classifying an AI system as high-risk [emphasis added]."

[80] Digitization is the process of changing information from analogue to digital form, and digitalization is the processes which involves the application of digital technologies to a wide range of existing tasks and enable the performance of new tasks, and include both the innovation process itself and a key driver of innovation. Katuu, Shadrack, *Management of public sector records in the digital age*, 2022, 2, Doi:10.13140/RG.2.2.25539.48163; Oslo Manual, 38.

[81] N. Haefner, J. Wincent, V. Parida and O. Gassmann, *Artificial intelligence and innovation management: A review, framework, and research agenda*, in *Technological Forecasting and Social Change*, vol. 162, 2021, 3, https://doi.org/10.1016/j.techfore.2020.120392.

[82] NHS, *A buyer's guide*, 5.

Because of this transformative nature, the public procurement of AI-driven solutions can be easily placed in the context of *public procurement of innovation*.

On the one hand, *innovation* consists of "a new or improved product or process (or combination thereof) that differs significantly from the unit's previous products or processes and that has been made available to potential users (product) or brought into use by the unit (process)".[83] In a nutshell, an innovation is a new idea or invention that has been implemented and launched (or is in the process of being launched) on the market.[84]

On the other hand, the public procurement of innovation refers to any procurement that has one or both of the following aspects: (i) buying the process of innovation – research and development services – with (partial) outcomes; (ii) buying the outcomes of innovation. In this process, the public buyer first describes its needs, thereby stimulating suppliers to develop innovative products, services or processes not yet on the market. Then, the public buyer acts as an early adopter and acquires a product, service or process that is new to the market or has substantially new features. Finally, the innovation fostered by AI may disrupt the existing ecosystem "by creating different actors, flows and values (disruptive innovation)", or it may even require a deeper transformation "involving structural or organisational reforms (transformative innovation)" if unmet needs arise.[85]

There is no general definition of healthcare innovation that covers all the legal, operational and clinical aspects of assessing the innovative nature of a device or product. The most relevant notion to qualify a healthcare innovation would appear to be: "the satisfaction of an unmet medical need". In the R&D phase, a healthcare product (a medical software) or procedure is considered innovative when it presents a novelty other than a simple technical evolution in relation to the existing healthcare technologies, making it possible to satisfy an unmet medical need. In the commercialization phase, new or significantly improved supplies or services are considered innovative. In addition, innovation procurement could target services relating to organizational innovation in patient care, quality of life for carers and caregivers, and the environmental footprint of healthcare products.[86]

Procurement can be used strategically to support the adoption of AI across government and rip off the benefit from economies of scale in the deployment of AI technologies.[87]

Obwegeser and Müller have provided a three-tiered classification to capture the relationship between innovation and public procurement: (1) public procurement for innovation (PPfI); (2) public procurement of innovations (PPoI), and (3) innovative public procurement (IPP).[88]

[83] OECD and Eurostat, Oslo Manual 2018: Guidelines for Collecting, Reporting and Using Data on Innovation. The Measurement of Scientific, Technological and Innovation Activities, 4th Edition, OECD Publishing, Paris/Eurostat, Luxembourg, 2018, 20, https://doi.org/10.1787/9789264304604-en. The OECD definition contains two key aspects: the innovation can cover both an activity and the result of the activity; and, the term "unit" describes the agent responsible for the innovation. See also Article 2(22) of the Directive 2014/24/EU which defines "innovation" as "the implementation of a new or significantly improved product, service or process, including but not limited to production, building or construction processes, a new marketing method, or a new organisational method in business practices, workplace organisation or external relations inter alia with the purpose of helping to solve societal challenges or to support the Europe 2020 strategy for smart, sustainable and inclusive growth".

[84] Observatoire Économique de la Commande Publique, *Guide Pratique. Achat Publique de Innovant*, Miniestère de l'Économie et des Finances, 2020, https://www.economie.gouv.fr. Therefore, an innovation must be distinguished from an invention by its operational nature: the innovation is about to be or has just been commercialised. At the crossroads between inventions and commercialised products is the work of Research and Development (R&D), which corresponds to all activities relating to fundamental research, applied research and experimental development, including the creation of technological demonstrations, with the exception of the creation and qualification of preproduction prototypes, tooling and industrial engineering, industrial design and manufacturing.

[85] European Commission, *Guidance on Innovation Procurement* (C(2021) 4320 final), Brussels 18 June 2021, 5.

[86] Ministère de la Santé et de la Prévention, *Guide opérationnel de l'acheteur d'innovation en santé. Préparer, contractualiser, exécuter, reporter les achats d'innovation en santé*, version 0, January 2023, 7, https://sante.gouv.fr.

[87] UK Guidelines, 13.

[88] N. Obwegeser and S.D. Müller, *Innovation and public procurement: Terminology, concepts, and applications* in *Technovation*, vols. 74-75, 2018, 4-5, https://doi.org/10.1016/j.technovation.2018.02.015. As to the authors, PPfI includes the use of public procuring by contracting authorities as a demand-side tool to drive innovation, i.e. as a part of innovation public policies; PPoI refers to the use of public procurement to innovate public services; and IPP is identified with models of innovative and ICT-enabled public procurement. While the third approach emphasises the potential uses of AI

By extrapolating these taxonomies into our analysis, a distinction can be drawn between public procurement as a demand-side tool to drive innovation for healthcare systems through AI (PPfAI), and public procurement of AI-enabled solutions to innovate NHCS (PPoAI).

Innovation-procurement strategies, i.e. public procurement of innovative solutions (PPI) and pre-commercial public procurement (PCP), can be placed under the umbrella of PPfI (Refs. [7] [11], [16], [17], [18], [20]), whereas the procurement of AI to enhanced and improve public-health services relates to PPoAI (Refs. [4], [5], [6], [8]-[10], [12], [15], [19]).

5.1. *Open-market consultations*

Considering the evolving and ever-changing nature of the market, the innovative dimension of the procurement decision to acquire AI software or apps for the NHCS, whether classified as medical devices or not, may face constraints due to a potential lack of comprehensive knowledge regarding existing solutions that are suitable to meet public needs.

By collaborating closely with companies, contracting authorities can verify that their criteria for quality, cost, deadlines, environmental and social performance are in proportion to the capacities and constraints of the sector concerned, and mitigate the risk of mismatches between supply and demand, thus reducing the likelihood of excessive costs, poor quality, or unsuccessful bids. [89]

Open market consultations (OMC) can help the contracting authority to determine whether potential innovations may satisfy the public need to be met and to identify potential vendors within a certain sector of the market.

In this sense, Article 40 of Directive 2014/24/EU allows contracting authorities to seek advice from independent experts or market participants. However, this should be done in a manner that avoids distorting competition and ensures compliance with the principles of non-discrimination and transparency. Moreover, in OMC on innovative procurement, the guarantee of confidentiality constitutes an insurmountable barrier.[90]

Therefore, conducting OMC could be a crucial strategy in innovation procurement in general and in AI for the healthcare sector in particular. National health services, with the assistance of the discussed multidisciplinary teams, should advocate for the adoption of an AI solution only if it proves to be the most suitable option for their requirements and after thorough assessment of all associated implementation risks.

In essence, the primary objective of conducting an OMC is to assess the state of the art before starting a procurement procedure in order to gain a comprehensive understanding of the relevant market. Preliminary market consultation allows the public buyer to achieve several key objectives:[91]

- To uncover creative ideas from the market;
- To define the conditions for addressing the challenge at hand;
- To foster opportunities for collaboration among market entities and with public buyers;
- To assess the organization's readiness to address opportunities and risks associated with innovation;
- To define and refine the subject-matter of the contract, including the best terms and conditions governing it.

There is no one-size-fits-all method for conducting market consultations. In certain instances, public purchasers may possess sufficient knowledge and only require clarifications or updates, while in other scenarios, more extensive research or analysis may be necessary to determine the appropriate definition of the AI solution to be procured.

Considering the substantial technical expertise demanded by both AI and the healthcare sector, OMC plays a crucial role in helping public purchasers determine the suitability of an AI approach. This involves evaluating the accessibility of relevant and representative data or the need to establish appropriate governance mechanisms for data management and sharing. Additionally, OMC

to innovate the procurement process (which is beyond the scope of this paper), the first and the second ones are very useful taxonomies for analysing the current state of art of the public procurement of AI-enabled solutions in the NHCS.

[89] Observatoire Économique de la Commande Publique, *Guide Pratique*, 10.

[90] M. Mesa Vila, *Fases de las licitaciones de compra pública de tecnología innovadora*, in *La compra pública de innovación en la contratación del sector privado*, J.A. Carrillo Donaire (coord.), INAP, Madrid, 2019, 55-56.

[91] C(2021) 4320 final, 38.

may help to identify core aspects of the technical specifications, such as data-quality requirements, bias avoidance, expected accuracy and performance levels, appropriate metrics, determination of use cases, maintenance and update obligations, compliance with technical standards, measures to ensure an ethical approach, milestones and deliverables, profile and skills of the teams in charge of the performance of the contract, etc.

Some tenders in the sample illustrate how PPI and PCP tenders are usually preceded by OMC.

For example, in the context of the third call of the FID Health Program by the Ministry of Science and Innovation (2019), the Health Department of the Autonomous Community of Madrid presented three projects for Public Procurement of Innovation that were favourably selected in November 2019, and received a 50% grant from the Pluri-regional European Regional Development Funds (ERDF) from the Spanish Ministry of Science and Innovation. The three Projects covered:

- MEDIOGENOMICS: Platform and expert system built on a SaaS approach, allowing the generation of clinical reports from raw genomic data from healthy/sick individuals, continuously updated to the state of the art, through the integration of AI-based software, to improve the efficiency and effectiveness of diagnosis, reducing time and sample handling.
- INTEGRA-CAM: A platform that enables home monitoring and follow-up of the intrinsic capacity of elderly people for early detection of disability or dependency situations, integrating patients, caregivers and healthcare professionals (primary and specialised care).
- INFOBANCO: Regional data-network architecture (Data Lake) enabling the collaborative exploitation of health data (clinical, research, and administrative) from various sources (primary care, hospitals, emergencies, pharmacy) to improve healthcare and innovation, value-based healthcare (VBHC), biomedical research, and other secondary uses.

The tendering of contracts INFOBANCO (Ref. [16]) and MEDIOGENOMICS (Ref. [17]) through their respective PPI procurement calls was preceded by a market consultation.

Market consultations in INFOBANCO and MEDIOGENOMICS Projects

Objectives of the OMC

- Receive proposals and innovative solutions that identify, specify, and evaluate both market needs and capabilities to delve into detailed solutions and proposals, leading to innovative and sustainable developments to achieve the goals set in each of the projects.
- Acquire sufficient knowledge about market capabilities and functional specifications that involve innovation and are feasible to be achieved through a potential Public Procurement of Innovation.
- Inform economic operators about the plans of the Health Department and the requirements they will be demanded to participate in the processes.
- Define the technical and administrative specifications for future PPI tenders.

Method and procedure:

- Publication of the call on the website of Health Department.
- Workshops and seminars with interested participants (more than 200 attendees). Presentation of the projects and questions from the participants.
- Participants had to fulfill a questionnaire describing their proposals, their elements of innovation (new technologies and innovative solutions), R+D expected outcomes, Technology Readiness Level (TRL) of the proposed solutions, intellectual-property-rights (IPR) limitations.
- Reception of the proposals in the time limit stipulated in the call.
- Interviews with some proponents to obtain further clarifications of the proposal in accordance with two relevant criteria: the functional approach and degree of innovation of the proposals.
- Examination of the proposals by an expert panel.

Common conclusions to be considered when drafting tender specifications:

- There were various solutions based on existing technology, although they did not fully meet the needs outlined and required by the Health Department. Therefore, innovative development was required to address the specific challenges of the three projects.
- The innovation proposals presented had an initial development ranging between TRL 6 and TRL 7, making the most suitable option to initiate a Public Procurement of Innovative Technology for the projects.

- Governance and data security were crucial points in all the projects due to their private and clinically-sensitive nature. Therefore, future specifications should consider compliance with GDPR, consent management, traceability systems, access, and related policies. - In relation to IPR, it was found that the model best suited to the projects was for the entity to keep the exclusive rights over the pre-existing base products provided by the entities under the contract. However, the IPR for any additional developments within the framework of the contract would be exclusive to the Health Department or shared between the Health Department and the entity.

Table 5. Open market consultations in innovation procurement for healthcare

5.2. *PPI and PCP strategies*

Where research and development (R&D) services are to be procured with a view to developing an innovative custom solution, public-health services will be able to procure research and development.

In cases where the public buyer retains exclusive rights to the benefits arising from R&D, including intellectual and property rights (IPR), the procurement of research-and-development services would fall within the scope of the public-procurement Directives. In turn, when the public buyer does not reserve all the benefits of the research and development services, such acquisitions would be exempt from the public-procurement Directives.[92] The first approach is PPI and the second is PCP.

As innovation procurement constitutes an administrative action to enhance R&D+i, implementing innovation-procurement strategies that combine PCP and PPI in a complementary way, public purchasers can drive innovation from the demand side.[93]

On the one hand, exempt from the application of public-procurement rules, PCP is characterised by competitive development in phases, risk-benefit sharing under market conditions, and separation from the deployment of commercial volumes of end-products/services.[94] It follows from the characterisation of PCP that this approach is used in those areas where existing solutions on the market do not meet a public buyer's needs.[95]

On the other hand, the deployment of commercial volumes of newly developed products and services would fall under the scope of the PPI. Consequently, PCP and PPI are complementary approaches.

PPI involves acquiring innovative solutions that do not require further R&D but are not yet available on a large-scale commercial basis. Nevertheless, they can be developed within a reasonable period of time, allowing for public-health services to perform compliance testing. In PPI, public purchasers act as early adopters or first buyers of innovative commercial end-solutions newly arriving on the market. It is also the best way to drive innovation and efficiency in public services. Hence, PPI involves the purchase of prototypes or the first complete products or services developed after the R&D phase, their testing and evaluation in order to select the best option before the final full-scale

[92] C(2021) 4320 final, 55.

[93] J.A. Carrillo Donaire and J. Tarancón Babío, *Concepto, sentido, objetivos y perspectivas de la compra pública de innovación*, in *La compra pública*, 17-19.

[94] Commission of the European Communities, *Pre-commercial Procurement: Driving innovation to ensure sustainable high quality public services in Europe*, COM(2007) 799 final, Brussels 14 December 2007; Pre-Commercial Procurement, Digital Strategy, last update 7 June 2022. https://digital-strategy.ec.europa.eu/en/policies/pre-commercial-procurement. In the first place, in PCP contracting authorities acquire R&D services from multiple competing suppliers simultaneously. This allows the comparison of alternative solution approaches and the identification of the most cost-effective solutions available in the market to meet the public needs. The R&D process is divided into phases, including solution design, prototyping, original development, and validation/testing of a limited set of initial products. The number of competing R&D suppliers decreases after each phase. Engagement in the initial phases of the R&D process allows public purchasers to identify potential policy and regulatory issues at an earlier stage. In the second place, risk-benefit sharing under market conditions is a key aspect of PCP. The risks (costs) and benefits (results) of the contract, including Intellectual Property Rights (IPRs) are shared between the public purchaser and companies under market conditions. This risk-benefit sharing encourages both parties to pursue widespread commercialization, the uptake of new solutions, standardization, and the publication of R&D results, thereby reducing the fragmentation of public demand. Finally, PCP is limited to the development and purchase of a restricted volume of initial products or services. This limitation is imposed because, in a service contracts like PCP, the total value of acquired supplies must remain below 50% of the overall PCP contract value. As PCP focuses on research and development, it does not encompass large-scale production for commercial volumes of end-products.

[95] C(2021) 4320 final, 56.

purchase.[96]

Depending on the specifications inherent to each product or service, PPI can be organized through regular procedures (open or restricted) and special procedures (negotiated tender, competitive dialogue, and partnership for innovation).[97]

Tenders in the sample show that both approaches have been used in the procurement of AI solutions for the NHCS. While PPI procurements were conducted in relation to contracts, PCP [11], [16], [17] was the strategy followed in [7], [18] and [20].

In the ROSIA project (Remote Rehabilitation Service for Isolated Areas), three public purchasers from Spain, Portugal and Ireland jointly sought the development of a comprehensive rehabilitation service enabling service providers to provide telerehabilitation, and self-management of rehabilitation & self-care at home, with a focus on remote areas by engaging patients and caregivers. To achieve this goal, the procurement process was preceded by an OMC seeking to collect comprehensive and detailed information related to existing experience, knowledge, solutions, budgetary constraints, and to provide feedback on the future PCP scope and phases.[98]

The project was divided into phases, which were further delineated across three consecutive PCP calls. Reference **[20]** in Annex II corresponds to Phase 1 of the entire project. Tender specifications included AI approaches, virtual reality and IoMT.[99]

The three PCPs in the ROSIA Project

The context

Contracting authorities participating in ROSIA were in urgent need of reorganising their rehabilitation services. The are tools already available in market, such as AI, virtual reality, augmented reality, gamification, depth cameras, sensors and IoMT, which have proven clinically effective in supporting telerehabilitation.

The challenges

However, telerehabilitation is a complex process:

- For the healthcare system. On the one hand, it implies an internal process of transformation towards specifically-tailored integrated-care models. On the other hand, handling the transference of sensitive data and integrating a large and diverse set of digital therapeutics into their own ICT systems.
- For developers. They face fragmented-care models, lack of prescribed procedures, and the diversity of ICT health systems to integrate. The costs of development are prohibitive.
- For patients. While having a significant impact on patients' lives and on their medical conditions, rehabilitation processes may have negative side effects on patients' lives when patients are forced to travel long distances to specialist rehabilitation centers (as is the case of patients living in remote and depopulated areas).

The PCP: unlocking tele-rehabilitation market

In this stand-off, a PCP process, where public procurers work in direct collaboration with the research capacity of the market, is in a unique position to unlock the situation.

ROSIA PCP was seeking to unlock the telerehabilitation market by purchasing the

[96] *Idem*, 58.

[97] J.A. Carrillo Donaire *et al*., *Concepto, sentido, objetivos*, 35.

[98] See Instituto Aragonés de Ciencias de la Salud, *ROSIA OMC Report,* PLACE, 31 March 2022, 33-39, 113, 117, available at https://contrataciondelestado.es/. Among the value-added proposals presented, some participants showed expertise on the application of AI in health status to support remote assessment and monitoring of physical function, prediction of falls and frailty, including neurorehabilitation tools based on virtual reality with AI tested in real environment with real patients; the development of AI medical devices with CE marking, or accountable AI. The OMC final Report made some recommendations for the future PCP in relation to:
Technology Readiness Level (TRL): The project was expected to start with a TRL of 5-6 and end with a TRL of 8-9.
Technological elements: ROSIA would be an open platform with trusted layers where services could share data, analysis and targeted interventions. As integration with the public health IT systems of three different countries is complex, the tender specifications should include the development of a sandbox that would allow a minimum set of data from the health systems of the three purchasers to be made available during the project to implement integrated care models.
Certification pathway: The tender specifications would include the implementation of a certification process for applications and devices included in the ROSIA catalogue, in line with the MDR.
IPR: While companies that were more reluctant to grant purchasers a free user licence seemed to have a better understanding of the clinical reality behind the ROSIA challenge (42%), those that promoted more open approaches seemed to require more clinical knowledge (58%). It was therefore recommended that representatives of both approaches should compete in ROSIA PCPs to compare outcomes, timescales and budgets.

[99] Instituto Aragonés de Ciencias de la Salud, *TD1-Request for tender*, PLACE, 11 May 2022, 17-31, *TD2 - Challenge Brief*, PLACE, 11 May 2023, 31-54, both available at https://contrataciondelestado.es.

development of a technological innovation ecosystem, enabling service providers to provide telerehabilitation, and self-management of rehabilitation & selfcare at home, at scale.
The ecosystem's design would allow flexible implementation of a value-based and integrated-care model, data driven intervention and the integration of third-party solutions.
The PCP proposed that the ROSIA Innovation Ecosystem be composed of three core elements that the 3 public purchasers could share across region:
- **ROSIA Open Catalogue**: A menu of evidence-based safe certified ICT solutions and services to be prescribed by a care team. All these services will allow the seamless sharing of clinical data with patients' consent.
- **ROSIA Developer Layer**: The development of architecture and layer for developers with open API's & governance tools to facilitate apps and services that uniformly can plug into the diverse backends of the buyer's regional infrastructures. This layer was expected to allow developing solutions based on existing modules and will aid existing research projects in becoming market solutions.
- **ROSIA Open Platform**: An open cloud-native platform to host shared services, communication, and manage Integrated Clinical Care Pathway builders, ePROM/ePROM protocol editor, data sharing, analytics, consent, login, business logic and other core shared services. The cloud platform could be provided privately or publicly as long as it complies with the ROSIA governance defined in the technical specifications (best practices and standards, openness, handover & education for each region, maintenance and updating).

The ROSIAS's PCPs
The project was split into three phases corresponding to consecutive PCP calls.
- **Phase 1. The solution design (PCP's Docket No. ROSIA PCP 101017606).** The selected contractors were asked to provide a solution design (architecture and components), including the governance approach; to determine the approach to be taken to develop ROSIA solution and/ or services needed, and to demonstrate the technical, financial; and commercial feasibility of the proposed concepts and approach to meet the procurement needs.
- **Phase 2. Prototyping (PCP's Docket No. PHASE 2 ROSIA PCP 101017606)**: In a first stage, the development, demonstration and validation under laboratory conditions of non-or-partial prototypes of key system components should take place. In a second stage, the prototypes would be designed as functional prototypes and would be expected to demonstrate component behaviour and system-wide interaction.
- **Phase 3. Field-testing (PCP's Docket No. PHASE 3 ROSIA PCP 101017606)**: In this final Phase, the prototypes would be used in the provision of care remotely, the Open Platform would seamlessly communicate to all enrolled users and to report and manage care for test individuals and selected pathologies. The validation of the ecosystem readiness with healthcare professional and patient users would include the deployment of sandbox-testing tools matching procurers ICT systems setting.

Table 6. Pre-commercial Procurement of AI for healthcare

5.3. *Choosing the appropriate procurement procedure for innovation*

The European Commission Guidelines on innovation procurement recommend public purchasers to use procurement procedures that do not prescribe a specific solution, but rather describe problems and needs, leaving room for suppliers to propose alternatives.

Therefore, the procurement of AI-driven solutions for healthcare should not be straightforward. The objective is not simply to obtain standardized products that align with conventional-procurement procedures, such as the open procedure, or the selection of the most economically-advantageous offer solely based on the economic criterion of price.[100]

Instead, there is a need for the adoption of more innovative procedures where the purchased solution is not rigidly defined in the specifications. In such cases, criteria such as quality and, notably, the ethical considerations of AI implementation could carry significant weight in the selection process for determining the most economically-advantageous offer.[101]

In consequence, to secure AI systems aligned with the public needs of the NHCS, public-health systems should employ "innovation friendly procurement procedures" (competitive procedures with negotiation,

[100] C(2021) 4320 final, 25.
[101] *Idem*, 42-44.

competitive dialogue, innovation partnerships)[102] when, for example, the needs of the contracting authority cannot be met without adaptation of readily available solutions or they include design or innovative solutions.[103] These procedures can facilitate the integration of new technologies, incorporate provisions for testing and prototyping before final procurement commitments, and foster collaboration among various bidders or encourage market participation in the exploration of alternative solutions.

If procedures that enhance market engagement or allow for contact and collaboration between procurers and bidders are inherent to the procurement of innovation, then open and restricted procedures should be discarded when procuring AI-driven innovative solutions.

Upon reviewing the tenders in the sample, the open procedure[104] emerges as dominant, having been applied in all (Refs. [1]-[4], [6]-[8], [12]-[20]) but four instances (Refs. [5], [10]-[11]). Regardless of the innovative nature of the AI-driven solutions or the lack of readily-available solutions in the market to meet specific needs, it is clear that the open procedure is the option preferred by public purchasers.

While special procedures (procedures with negotiation, competitive dialogue, innovation partnerships) are better suited to innovation procurement, the clear preference of purchasers for the open procedure may be due to the greater legal certainty and control over deadlines and timing on the one hand, and the lower complexity, duration and fewer resources needed on the other.[105]

All specific procedures in the sampled tenders have been utilized, except for the innovation partnership.

Leaving aside the risks of vendor lock-in or the fact that the continuous learning of some AI models could change the intended purpose of the contract, open procedures may work better for standardised products available in the market. However, this will not be the case for many of the contracts in the sample, as the public needs to be met are associated with specific use cases for which the market has not yet provided COTS solutions. The call for tender launched by Red.es is an example of application of AI solutions to use cases pre-defined by the tender specifications (Ref. **[13]**).[106]

AI solutions for 15 use cases in the Healthcare System of Andalucia

The context

As part of the Primary Care Renewal Strategy, the Andalusian Health Service (SSPA) developed a Population Health Database with traditional analytical capabilities.

The challenge

The SSPA aimed to apply advanced analytics with AI, including ML and DL approaches, to enable massive-information exploitation from the Population Health Database and overcome the technological limitations of the traditional Business Intelligence environment.

The use cases described in the technical specifications

It was expected that the prospective contractor would provide an on-premise software and hardware platform with the capability to hybridize with the cloud. This platform is intended for the development and deployment of AI-driven solutions, to be applied in at least 13 use cases listed below:

1. Defining factors that influence morbidity and predicting associated future health risks.
2. Designing optimal pathways and personalisation in the provision of health services.
3. Optimising the distribution of quotas in primary care based on the frequency of visits, the time spent per visit, the complexity of visits and/or patients, the number of pathologies or chronicity.
4. Segmenting chronic patients, across a pre-defined population, based on the level of care required.
5. Comparing the results of pharmacological treatments in pathologies of the same type.
6. Using predictive models for the evolution of population groups in terms of health-resource consumption.
7. Recommending engine to optimise the surgery waiting list.
8. Identifying and preventing drug-drug interactions that may cause health risks in poly-medicated patients.
9. Identifying target patients for new pharmacological treatments.

[102] *Idem*, 52.
[103] Cfr. Article 26(4)(a) of the Directive 2014/24/EU; Article 31, paragraph 2.
[104] Article 27 of the Directive 2014/24/EU.
[105] M. Mesa Vila, *Fases de las licitaciones*, 60.
[106] See Red.es, *Pliego de Prescripciones Técnicas*, 4-5, 13, 84-93.

10. Using radiological image analysis to support breast cancer screening. 11. Processing clinical text using NLP technologies to develop a CIE10 and SNOMED codifier. 12. Detecting public-health alerts based on social-network analysis. 13. Optimising hospital contingency plans to reduce surgical waiting lists or waiting times for hospital specialists by predicting the availability of hospital beds and staff or the need for healthcare resources. 14. Predicting demand for services in private centres as part of a hospital agreement with the regional public health system. 15. Identifying factors that can predict sepsis in patients.

Table 7. AI COTS solutions aligned with pre-defined use cases in healthcare

In the same vein, the 'MedP Big Data' project, launched by the Regional Governments of Gran Canarias and Valencia, sought the design of AI algorithms, a patient-healthcare system interface, support tools for clinical decision-making, and a hybrid platform that operates both on the cloud and on-site upon request. The objective was to apply these solutions to a wide range of use cases (almost 20), with a special focus on chronic pathologies of oncological and cardiovascular nature, and optimising protocols in advanced cases, both for individual diagnosis and treatment and for population and research settings.[107]

A key factor influencing the decision between applying a procedure with negotiation or opting for competitive dialogue is the level of definition of the subject matter that the public purchaser intends to procure.[108] In the context of public procurement for AI solutions in healthcare, the former scenario involves a contracting authority with a precise understanding of the nature, elements, features, and functionalities of the solution. Conversely, in the latter case, the subject matter of the contract is less defined, and the contracting authority lacks sufficient knowledge about the optimal way to address the public need. Consequently, in such instances, the authority relies on the market to present available choices in advance.

Tender procedures with negotiation will offer public health-service authorities the possibility to award these contracts with greater flexibility, particularly in cases where off-the-shelf AI-solutions are unavailable in the market or where the negotiation process allows public buyers to negotiate adaptations of existing elements or conditions for the development of an innovative solution. In the procurement of the assistant system, AVATAR, the Regional Healthcare System of Galizia justified the application of the procedure with negotiation (Ref. **[9]**).[109]

AVATAR
The state of the art in the market There are already numerous technological solutions aimed at improving health available in the market for various pathologies, thanks to the development of mobile applications linked to sensors. **The challenge** One of the most significant needs in healthcare processes is to enhance and strengthen communication between healthcare professionals and patients, especially where a significant health problem or risk is detected, requiring prompt action. In such cases, the information to be communicated serves as a warning or alert. **The enhanced solution: justifying the**

[107] Gobierno de Canarias and Generalitat Valenciana, *Pliego de Prescripciones Técnicas para la Contratación de un Servicio de I+D del Proyecto "Medicina Personalizada Big Data", mediante Procedimiento Abierto de Adjudicación y Tramitación Ordinaria, Tipo Compra Pública Precomercial*, 28 December 2021, 5,6, 18-29. Use cases described in the tender specifications covered, inter alia: the application of NLP in the domain of clinical reports using semantic tagging SNOMED CT; description of lumbar pain pathophysiology through the application of predictive-analytics techniques based on medical imaging with magnetic resonance; home monitoring of chronic situations and hospital discharges, with reference to oncology patients undergoing treatment in day hospitals and home hospitalization, and application in other related cases (patients in the first month post-hospital discharge, in home palliative care; or patients with diabetes mellitus, psychopathologies, EPOC, chronic pain, among other pathologies); patient segmentation in the most relevant pathologies; measurement and prediction model of the efficiency of primary-care functional units; patient selection for clinical trials and for active search for rare diseases; prediction of unplanned readmissions in the month.

[108] M. Mesa Vila, *Fases de las licitaciones*, 61.

[109] SERGAS, *Informe del Servicio Promotor para la Contratación mediante la Modalidad de Compra Pública de Tecnología Innovadora por el Procedimiento de Licitación con Negociación, del Servicio de Desarrollo y Fase Demostración de un Sistema de Asistente Personal (AVATAR) y un Generador de Alertas Inteligentes que aumente la Autonomía del Paciente*, 6 September 2018, 7; and, *Pliego de Prescripciones Técnicas*, 31 August 2018, 9-10, https://www.contratosdegalicia.gal/.

procurement with negotiation
The project aimed to address these two components collectively: the improvement and optimization of bidirectional communication among patients, professionals, and caregivers, combined with the management of warnings and alerts generated in the monitoring process of patients' biological or behavioural parameters. The design of the solution should particularly consider the needs of individuals with communication difficulties (persons within the autism spectrum, with neurodegenerative diseases, with visual, auditory, mobility impairments). This enhancement of communication could be achieved through augmented reality, personalized avatars, text-to-voice systems, etc. The tender specifications, in particular, emphasized the use of avatars, as they enable the visualization of our health in the future or improve understanding of how to treat a disease through new treatments by simulating different alternatives.

Table 8. Procedure with negotiation for an AI solution

A specific derogation, contained in Article 32(3)(a) of Directive 2014/24/EU, allows the use of a negotiated procedure without prior publication for the procurement of research and development supplies. The products or services procured must be supplied exclusively for the purpose of research, experiment, study or development, and the contract shall not include series production aimed at establishing commercial viability or amortising research-and-development costs.

Under Article 32(3) (b) of the Directive, this procedure can also be applied where supplies or services can be supplied only by a particular economic operator for any of the reasons established by the Directive, *inter alia*, the lack of competition for technical reasons, or the protection of exclusive rights, including intellectual-property rights. In this sense, the apparent lack of competition in the application of differential privacy and NLP to the processing of health records and the protection of exclusive IPR of a legacy-proprietary software seems to be behind the application of the negotiated procedure without prior publication in the procurement of the advanced expert-healthcare AI-support system for the exploitation of the Hospital Infanta Leonor's electronic medical records (Ref [9]).[110]

Competitive dialogue is a procedure consisting of two rounds, whereby the contracting authority describes its needs in a descriptive document or a contract notice, establishes the minimum requirements for candidates and defines the criteria for awarding the contract on the basis of the Best Price Quality Ratio (BPQR).[111]

Upon confirming candidates' adherence to the selection criteria, the buyer commences a competitive dialogue with those meeting the minimum requirements in order to determine the feasibility and suitability of the solution. Individual negotiations are carried out with each candidate, prioritizing the confidentiality of their respective solutions. This demands a significant level of technical proficiency from the public purchaser's team and considerable time investment. Establishing milestones serves to evaluate negotiation progress and eventually streamline the candidate shortlisting process over time.[112]

Competitive dialogue provides an opportunity to discuss and define with the candidates the appropriate technical or financial solution, which the public authority is not in a position to define alone and in advance. This procedure facilitates an iterative co-building process with suppliers to develop a technical solution that best aligns with the requirements of the public purchaser. This approach goes beyond exclusive-price negotiations, providing an avenue to explore innovation possibilities collaboratively with suppliers.[113]

While the innovative character of the competitive dialogue may consist of technical, financial or administrative aspects, or a complete reorganisation of the public purchaser's operational process, the use of this procedure for the procurement of AI solutions usually relies on the technical aspects of the challenges.

[110] Hospital Universitario Infanta Leonor, I*nforme justificativo del procedimiento negociado sin publicidad en la adjudicación del contrato de servicios titulado: "Evolución, soporte y mantenimiento de un sistema experto avanzado de apoyo a la atención sanitaria, implementado con inteligencia artificial, para la explotación de la información (Big data) contenida en el conjunto de las historias clínicas electrónicas del Hospital Universitario Infanta Leonor*, 22 July 2019, 1-2, https://contratos-publicos.comunidad.madrid/.

[111] C(2021) 4320 final, 53.

[112] *Ibidem*.

[113] Ministère de la Santé et de la Prévention, *Guide opérationnel*, 28-29.

For example, one of the largest health trusts in Norway launched the AIRad project in early 2020 to procure and implement ready-to-use commercial AI solutions to optimise the screening of computer tomography, magnetic resonance and X-ray images, and match them with an algorithm-detected pathology for quicker follow-up. Due to the complexity of the tender, the contracting authority used a competitive-dialogue procedure to develop the specifications in collaboration with the vendors involved. The dialogue-based tendering process sought to (i) overcome the difficulties of relying on algorithms that had not been validated on data from the Health Trust's own patient population, (ii) compare the pros and cons of acquiring CE-marked single-algorithm vendors or platform solutions for testing, validating and tailoring AI models to specific use cases prior to implementation in clinical practice, and (iii) ensure appropriate integration with the Trust's existing infrastructure and organisational practices.[114]

Further examples of the competitive dialogue can be found in the tenders of Annexes I and II: the AI-driven platform for Primary Health Care (Ref [4])[115] launched by the AGENAS and the CADIA project for a support system for cancer detection based on imaging screening with AI techniques procured by the SERGAS (Ref. [11]).

Justification of the competitive dialogue in CADIA
- Addressing the needs identified by the contracting authority that cannot be fulfilled through existing solutions in the market. Then, it is deemed necessary for bidders to undertake prior design or adaptation work. - The contract encompasses services that involve the integration of innovative solutions. - The service requirements are rooted in emerging technologies, specifically AI techniques. The technical specifications cannot be precisely established by reference to a standard, European Technical Assessment, Common Technical Specification, or technical reference.

Table 9. Competitive dialogue for an AI solution

6. *Planning AI procurement for the NHCS: 'what to buy'*

AI public procurement is not exempt from challenges that affect the entire procurement process, from the preparation of the tender (preliminary engagement with the market if appropriate, identification of specific needs to be met with the contract, design of the specifications, and development of the procurement procedure) to the execution of the contract and the establishment of appropriate controls.

Due to the disruptive and evolving nature of AI and its potential impacts on healthcare, contracting authorities should consider some specific guidelines to guide their procurement procedures, not only from the perspective of the strategic use of public procurement as a tool for innovation in NHCS, but also as a tool to ensure the acquisition of trustworthy solutions.

6.1. *Alignment with national or regional strategies for AI adoption in NHS*

Contracting authorities should align their AI procurement with relevant national or regional AI-strategy initiatives and guidelines from agencies that inform government policies on new technologies. Before engaging in an AI deployment, contracting authorities should consider how their pursuit of an AI system aligns with their overall national or regional strategies. This allows contracting authorities to incorporate secondary policy objectives into their strategic procurement, potentially leveraging economies of scale by aggregating demand for AI systems.[116]

An additional benefit of aligning with a

[114] L. Silsand *et al.*, *Procurement of artificial intelligence for radiology*, 1388-1395.

[115] AGENAS, *Avviso di indizione di una procedura di dialogo competitivo per l'affidamento di un contratto avente ad oggetto la progettazione di dettaglio, la realizzazione, la messa in esercizio e la gestione di una piattaforma di Intelligenza Artificiale*, 21 October 2022, https://www.agenas.gov.it/. Pursuant to the Decision no. 5 of 9 January 2024, the AGENAS temporarily and precautionarily suspended the competitive dialogue procedure following a formal request for information by the Italian Data Protection Authority, Il Garante per la Protezione dei Dati Personali. The request of the Il Garante sought clarification on the legal basis of the processing, the technical and organizational measures to implement data protection by design and by default principles across the platform, and the methodology to implement the "Decalogo per la realizzazione di servizi sanitari nazionali attraverso sistemi di Intelligenza Artificiale" of September 2023 passed by Il Garante. Network Digital 360, *Piattaforma di intelligenza artificiale per l'assistenza sanitaria: al via la fase finale della procedura per la realizzazione. Aggiornamento: gara sospesa*, 22 January 2024, www.healthtech360.it.

[116] UK Guidelines, 13.

national or regional AI strategy is that there may be specific support for initiatives that align with the strategy, such as access to additional experts. To improve their practices, contracting authorities could actively seek collaboration across departments and disciplines. Contracting authorities could also share knowledge and feedback through expert communities, such as the digital purchasing community, professional networks or meet-ups. Within the department or unit responsible for procurement, it could be helpful to set up platforms and networks to share information, experiences and best practices on buying AI-enabled solutions.[117]

In the case of the tenders corresponding to Spain, with some exceptions, there is a general absence of specific national or regional AI strategies in the health sector.

In accordance with Decision SLT/954/2023 of 19 March, the Government of Catalonia has published the Programme for the Promotion and Development of Artificial Intelligence in Health ("Health/AI Programme"). The aim of the programme is to create an enabling environment for innovation in the Catalan health sector through the development and implementation of AI solutions to improve the health of citizens, using the knowledge generated by the Catalan Public Health System (SISCAT). In doing so, Health/AI Programme seeks to prioritise prevention and improve the quality of care and sustainability of the health system. The goals of the Programme do emphasise the importance of the transfer of knowledge, trustworthy and verified AI solutions, the strategic alignment with overall healthcare planning, public procurement for public value, and true engagement of relevant stakeholders. Accordingly, the Health/AI programme functions include:[118]

- Strengthening the health AI ecosystem by supporting research, development and innovation that facilitates knowledge transfer to SISCAT to increase its capacity to develop AI.
- Adopting innovation as a catalyst for the implementation of AI according to assessment methodologies at clinical, ethical, legal and technological levels before implementation in SISCAT and verification of the functioning and impact of the algorithms by experts in different fields of knowledge.
- Promoting the improvement of SISCAT efficiency by developing AI solutions on a systemic scale to optimise human welfare, provided that all evaluation criteria guaranteeing the reliability of the solutions are met.
- Facilitating the strategic alignment of all relevant stakeholders in response to the overall policies and priorities of SISCAT, as defined in the Catalan Health Plan.
- Ensuring that the processes of procurement and implementation of AI in the health sector progress and establish a broader vision of AI that enables innovation systems of public value.
- Encouraging the participation and involvement of the entire Catalan health system to ensure a significant improvement in the quality of information and the achievement of results with a greater impact on the whole system with the resources allocated.

The tender specifications of some of the annexed contracts are contextualised with European, national or regional strategies linked to specific components of National Recovery and Resilience Plans of the Next Generation Funds devoted to the eHealth and the use of AI for personalised medicine services (Refs. [4], [5], [15]).

In accordance to the corresponding specifications, the Telemedicine platform procured by the Italian Agency, AGENAS (Ref. [5]), was aligned with: (i) the Italian Recovery and Resilience Plan (Mission 6, Component 1, sub-investment 1.2.3 "Telemedicine"); (ii) the European Health Data Space, a key pillar of the strong European Health Union (European Commission's EU Global Health Strategy 2022) and it is the first common EU data space in a specific area to emerge from the European Strategy for Data 2020.

In the same vein, the Spanish Ministry of Health (Ref. [15]) sought to procure development applications for the digital transformation of the National Health System, including the implementation of AI and NLP-driven analytical tools, along with other data-driven technologies such as big data,

[117] WEF Guidelines, 10.

[118] Departament de Salut, *RESOLUCIÓ SLT/954/2023, de 19 de març, per la qual es crea el Programa per a la promoció i desenvolupament de la intelligència artificial al sistema de salut*, Official Gazette of the Generalitat de Catalunya, no. 8881, 23 March 2023, https://portaldogc.gencat.cat.

blockchain and robotics. The contract was framed within the Spanish Digital Health Strategy of the NHCS of 2021, which is linked to the National Plan for Recovery, Transformation and Resilience, and several Spanish digital strategies (Digital Spain 2025, Science, Technology and Innovation Strategy, Artificial Intelligence Strategy, Personalised Medicine Strategy).

It is important for contracting authorities to ensure that their technology and data strategies are updated to incorporate the use of AI technologies. Consideration should be given to aligning the work of contracting authorities with other teams in central or regional government departments and organisations that are leading relevant AI initiatives, and establishing networks to share insights and learn from best practice.[119] In this sense, Directive 2014/24/EU does not prevent the practices of joint procurement between contracting authorities.[120]

An example of joint procurement is the project ROSIA (Ref. [20]), where the lead procurer, the Institute of Health Science of Aragón (IACS) acted on behalf of the Buyers Group, which was composed by VALDE INNOVA (Spain), Instituto Pedro Nunes (Portugal), The International Foundation for Integrated Care (The Netherlands), The Decision Group (The Netherlands), Instituto para la Experiencia del Paciente (Spain), PPCN.xyz Aps (Denmark) and the Municipalities of Penela and Soure (Portugal). In the same line, the European Food Safety Authority (EFSA) and other EU bodies jointly sought assistance for statistical and epidemiological analyses using AI methodology (Ref. [2]), and the Governments of Gran Canaria and Valencia also launched a joint procurement (Ref. [18]).

6.2. *The expertise of the contracting authority: the need of multidisciplinary teams*

Many contracting authorities may be faced with a lack of skilled and multidisciplinary teams to conduct the appropriate analysis of whether or not an AI system is the optimal solution to meet a public need. There are inherent risks in this, insofar as the authority can be prone to rely on vendors or private consultants that could "shape the framing of the need, or even create the perception of a need in the first place, which then kicks off the procurement process".[121]

To avoid such risks, most international and national standards for AI procurement emphasise the need for multidisciplinary teams covering all areas of knowledge that may be affected by the implementation of AI solutions. That is, specialists in medical science, computer science, data engineering, the applicable legal regime or ethics. In addition, such teams should be encouraged to have expertise in the design, procurement, operation and control of AI systems.

Only in the absence of such experience or the appropriate profiles, external assistance may be contracted to fill the existing gaps. At this point, it is important to highlight the necessary presence of lawyers who must not only be the architects of the contracting procedure,[122] but must also play a fundamental role in ensuring that the solution to be implemented complies with all applicable regulations without infringing patients' rights. In this sense, lawyers will have to work together with other experts to enrich the process of integrating AI into national health systems.

The lack of technical expertise is of particular concern when contracting authorities choose to purchase third-party AI software and hardware, including off-the-shelf AI models, AI-as-a-Service (AIaaS), AI Platform-as-a-Service (AIPaaS). This option could lead to vendor lock-in effects and also increase associated risks if contracting authorities do not fully understand the model (or the data it uses), do not have sufficient control over risks (such as managing data bias, addressing model explicability, or optimising performance), or become overly reliant on AI or overly confident in the accuracy of AI.[123]

6.3. *Conducting prior AI impact assessment*

Conducting initial AI impact assessments in a systematic way at the beginning of the procurement process, and ensuring that their

[119] UK Guidelines, 13.
[120] Recital (71) of the Directive 2014/24/EU.
[121] M. Sloane *et al*., *AI and Procurement*, 10.
[122] I. Gallego Córcoles, *La contratación pública como impulsor y garante del uso de soluciones basadas en inteligencia artificial*, in E. Gamero Casado (dir.), *Inteligencia artificial y sector público. Retos, límites y medios*, Valencia, Tirant lo Blanch, 2023, 524.
[123] Cfr. Bank of England, *FS2/23 – Artificial Intelligence and Machine Learning. Feedback statement 2/23*, 26 October 2023, https://www.bankofengland.co.uk.

preliminary findings inform the procurement, will be critical prior to the acquisition of an AI system. Impact assessments provide a better understanding of the potential impact of using AI and the ways in which potential risks can be mitigated. A team with diverse skills should support the contracting authority in conducting impact assessments and ensuring that the use cases and procurement process reflect their key findings.[124]

According to the Office for Artificial Intelligence in the UK, an AI impact assessment should reflect:[125]

1. The needs of the contracting authority and the public benefit of the AI system.
2. Human and socio-economic impacts of the AI system.
3. (Unintended) consequences for the existing technical and procedural environment.
4. Data quality and any potential inaccuracy or bias.
5. Any potential unintended consequences.
6. Whole-of-life cost considerations, including ongoing support and maintenance requirements.
7. Associated risk and mitigation strategies, including key point of the 'go/no go' decision where applicable.

In its protocol for the implementation of algorithmic systems in municipal services, and applicable to public procurement, the City of Barcelona provides for a mandatory, but non-binding, impact assessment of algorithmic high-risk systems from the very moment the service is conceived. This assessment will be carried out by an Advisory Board on Artificial Intelligence, Ethics, and Digital Rights, and will include the following information related to the algorithmic system to be tendered: description, purpose, scope, policy, and timeline for use; description of the application context; necessity and proportionality of the system; identification of parties involved; ethical review, including values and conflicts (trade-offs); impact on fundamental rights of affected individuals and communities; human oversight; definition of potential risks, mitigation measures; and recommendations.[126]

Importantly, there are examples of risk-assessment methodologies for automated decision making, such as the Government of Canada's Directive on Automated Decision Making. The "Algorithmic Impact Assessment (AIA)" is a self-assessment tool that allows Canadian departments and agencies to better understand and manage the risks associated with the implementation of automated decision systems. The tool consists of 51 risk and 34 mitigation questions, and provides a raw impact score based on based on several factors (system's design, algorithm, decision type, impact and data) and a mitigation score based on organisational and technical measures (consultations with internal and external stakeholders and de-risking and mitigation measures related to data quality, procedural fairness, and privacy).[127] To further transparency and trustworthiness of implemented AI systems, the Open Government Portal makes it publicly available the completed AIAs of various public bodies. Accordingly, the Portal has published AIAs in the area of healthcare.[128]

For its part, the European Law Institute has produced a set of model rules with procedural and substantive provisions for conducting impact assessments of algorithmic decision-making systems, including an extended questionnaire for completing the Impact Assessment Report.[129] The model rules cover, *inter alia*, the conditions triggering the application of an impact assessment, coordination with other impact-assessment procedures, initial risk evaluation (screening procedure) for systems not subject to a mandatory impact assessment, the content of the impact-assessment report, specific provisions for high-risk systems, publication of the assessment and iterative review, and accountability mechanisms. The proposed content of the impact assessment shows a clear alignment with the EU HLEG Guidelines and the AIA. The content of the impact assessment and the extended questionnaire can be adapted for its implementation in the procurement process of AI solutions for the NCHS.

[124] UK Guidelines, 24; WEF Guidelines, 8-9.
[125] UK Guidelines, 26.
[126] Barcelona Methodologies, 14-15.
[127] Government of Canada, *Algorithmic Impact Assessment tool*, last update 25 April 2023, https://www.canada.ca.
[128] Veterans Affairs Canada, Algorithmic Impact Assessment Results - Mental Health Benefit, 9 December 2022; Public Health Agency of Canada, Algorithmic Impact Assessment - ArriveCAN Proof of Vaccination Recognition, 27 October 2021, https://open.canada.ca.
[129] European Law Institute, *Model Rules on Impact Assessment of Algorithmic Decision-Making Systems Used by Public Administration*, Vienna, 2022, 16-51.

Scope and content of the AI Impact Assessment	
Provisions (Article 6 of the Model Rules)	**AIA (Articles)**
Description of the purpose and operation of the system	
Development of the system, in particular its algorithms.	11 Annex IV
Nature and technical characteristics of the system.	
Selection of training, validation and testing data.	
Context in which the system is used, in particular the public needs to be meet.	
System's interrelation with other digital systems (internal or external).	
Assessment of the performance, effectiveness and efficiency of the system	
In particular, whether the performance of the system might be flawed by low-quality data during its use.	13(3)(b)(iv), (4)
Assessment of the specific and systemic impact of the system on…	
Fundamental or other individual rights/interests (esp. rights to privacy and data protection, non-discrimination).	13(3)(b)(iii)
Societal and environmental well-being.	
End-user contracting authority, acceptance of the system/decisions by the staff, risks of over/under-reliance on the system, level of digital literacy, and technical skills within the authority.	14(4)
Assessment of the measures taken to ensure	
Maximisation of benefits to be achieved by the system with regard to public needs.	
Minimisation of identified risks and mitigation of possible negative outcomes.	14(2)
Human agency, oversight and control of the system.	14(1)(3)
High-quality data.	10
Accuracy across groups, precision and sensitivity.	15(2)(3)
Technical robustness and safety; resilience to attacks; data security; fall-back plans; reliability; and replicability of decisions.	15(3)(4)
Transparency of the system and explainability of its decisions.	
Traceability to enable the monitoring of the system's operations.	12
Accountability, in particular oversight, auditability, clear allocation of responsibilities, self-monitoring, benchmarking, and possibility of redress for injury or harm caused by the system.	17
Final determination of the risk level, unless the system is listed as 'high risk'.	9
Overall assessment of necessity and proportionality of processing operations in relation to the purposes, (esp. trade-offs between different factors considered in the impact assessment and reasonable alternatives to the envisaged system).	Annex IV (2)(b)
Reasoned statement on the legality of the use of the system under the applicable law, esp. data-protection law, administrative law and sectoral legislation	
Any additional information	

Table 10. Methodology for an AI Impact Assessment

As the disproportionate individual and social impacts of AI systems become more apparent, there is also a pressing need to introduce in the procurement process iterative risk and impact assessments, which importantly should include not only an *ex-ante* evaluation before starting the tender, but also during the post-implementation maintenance.[130]

In this sense, as part of this iterative approach to risk throughout the lifecycle of the public contract, contracting authorities should regularly review the assessments and their key findings,[131] taking into account any 'substantial modifications' to the intended purpose of the contract that may occur.[132]

[130] Cfr. M. Sloane *et al.*, *AI and Procurement*, 22.
[131] UK Guidelines, 14.
[132] See European Commission's Standard Contractual Clauses, 3. The document defines a "substantial modification" as "a change to the AI System following the Delivery which affects the compliance of the AI System with the requirements set out in these Clauses or results in a modification to the Intended Purpose" (Article 1.1). According to the contractual clauses of the Commission, there are some specific obligations addressed to document substantial modifications that may happen during the life cycle of the contract. In particular, the contractor must update the technical documentation and the in-

A review of the tenders of interest found no evidence that any AI-impact assessment was conducted before the tender notice was submitted, or that it was required in tender specifications. Even though most of the tenders implied systematic processing of large amounts of health data with a new technology –such as AI– , just only a few of them required a DPIA among the contractual obligations of the supplier (Refs. [4], [5], [13], [16], [18], [20]). Furthermore, in certain cases, there is no requirement for the supplier to furnish a DPIA when the contract purpose is to enhance legacy systems with new AI modules that could affect data processing (Ref. [9]).

6.4. *Building a credible use case for health care: Is AI the right solution?*

Neither EU public procurement rules nor Member States' national laws say what a public body "has to buy". Specifically, Directive 2014/24/EU makes it clear that nothing therein "obliges Member States to contract out or externalise the provision of services that they wish to provide themselves or to organise by means other than public contracts".[133]

Then, one of the problematic challenges in NHCS is the difficulty for contracting authorities of NHCS "to understand the *need* that is intended to be addressed and what, among many possible trade-offs, is the best solution". The reasons for this are due to the uncertainty and urgency of medical practice, risks of over or under provision, specificity of goods or services being purchased, barriers to market entry for new products, lack of health workers with appropriate skills, and asymmetry of information in favour of providers to the detriment of purchasers.[134]

The purchasing decision starts with a clear identification by the contracting authority of the public need to be met. It is easy for public purchasers to "overlook this critical step" due to the novelty and lack of awareness of AI technologies.[135]

An unmet need may arise from: (i) a problem that negatively impacts the delivery of the public service; (ii) a need or desire of a public purchaser to improve the quality and/or efficiency of the public service or a new emerging operational requirement; (iii) policy objectives to address medium to long-term societal challenges; (iv) legislative/regulatory requirements to deliver higher quality/efficiency public services.[136] If the notion of "acquisition" is broadly understood in the sense of "obtaining the benefits of the works, supplies or services in question",[137] the public need to be met by the contract should reflect the benefits of the public contract for the public service to be delivered by the public entity responsible of the service. The public need shall be aligned with the goals of the sector recognised in public-health policies, and particularly, with the improvement in health (including equitable improvement) and responsiveness to the legitimate expectations of users and societies.[138]

Moving forward, once the public need and the problem/challenge have been identified, the contracting authority must articulate the rationale behind the decision of choosing AI. There is an essential premise that purchasers need to consider: AI is not a one-size-fits-all or general-purpose solution that can solve every single problem. This basically means that, for the time being, current applications of AI are focused on performing narrowly-defined tasks. Whilst AI can help public bodies meet public needs, other, simpler solutions may be more effective, less risky and less expensive.[139]

When assessing if AI could help to meet the public need, NCHS contracting authorities should consider whether: (i) the problem to solve is associated with a large quantity of data which an AI strategy could learn from; (ii) analysing data would be so large and repetitive that it would be difficult for humans

structions for use at least with every substantial modification during the term of the contract, and subsequently make them available to the contracting authority (Article 4.4). Additionally, the automatic recording of log events shall include the identification of situations that may lead to any substantial modification in order to ensure an appropriate level of traceability of the AI System's (Article 5.2.b).

[133] Recital (5) Recital (4) of the Directive 2014/24/EU.

[134] European Commission, Public procurement in healthcare systems, 12-14.

[135] UK NHS Buyer's guide, 20.

[136] Cfr. European Assistance for Innovation Procurement, *The EAFIP toolkit on innovation procurement. Module 2*, Version 2021-2, European Commission, 2021, 1, 8-21.

[137] Recital (4) of the Directive 2014/24/EU.

[138] European Commission, Public procurement in healthcare systems, 77.

[139] Office for Artificial Intelligence and Government Digital Service, *A guide to using artificial intelligence in the public sector*, 27 January 2020, 1, 10, https://www.gov.uk/.

to do it effectively and efficiently; (iii) the outputs can be tested against empirical evidence to ensure the accuracy of the model; (iv) model outputs would lead to problem-solving in the real world; the datasets in question are available –even if preprocessing is required– and can be used ethically and safely.[140]

The European Centre for Disease Prevention and Control (ECDC) is a public health agency of the European Union (EU) which assesses risks and provides appropriate guidance to help countries prevent and respond to outbreaks and public-health threats. Through its mandate, the ECDC collects, analyses, and disseminates data on over 50 infectious disease concerns (e.g., COVID-19, influenza, HIV/AIDS, hepatitis, measles, tuberculosis, antimicrobial resistance). The ECDC's legal framework and its Strategy 2021-2027 prioritize the early detection and response to public-health threats as its core activities. The Agency launched a call for tender to support ECDC's utilization of AI strategies, encompassing ML and DL, in its surveillance procedures and other essential public-health duties. Additionally, the aim of the tender was to enhance the early detection of public-health risks through social-media channels, related training of learning models required to properly handle and sustain these outputs.[141]

EUROPEAN CENTRE FOR DISEASE PREVENTION AND CONTROL (ECDC)
2. Technical specifications **2.1. General background** Article 14 of Regulation (EU) 2022/2371 on serious cross-border threats to health defines the need to ensure the "continued development of the digital platform for surveillance", including the application of "artificial intelligence for data validation, analysis and automated reporting, including statistical reporting". ECDC detects public-health threats though its Epidemic Intelligence (El) processes, which include monitoring on a routine basis some epidemiological indicators for specific diseases (COVID-19, dengue, cholera, measles) and social-media platforms as a source of early detection of public-health threats. This monitoring has different challenges, including increased number of sources, changes in the sources, large amount of data and formats for extracting the data (e.g., text, images or video). As of 2022, automatization of EI processes is mainly based on the use of R programming, with sporadic use of other technologies (Scala and Python), which has required increasing the capacity on this type of technology for its sustainable use and maintenance. ECDC aims to further improve the efficiency and timeliness of EI activities as well as activities in other areas of surveillance and other core public-health functions through the application of AI, including automatization of processes, ML and DL algorithms and NLP.

Table 11. Assessing the public need of AI solutions in public-health surveillance

7. *Key challenges in formulating AI tender specifications for the NHCS*

Drafting tender specifications could be challenging, as it is necessary to avoid potential tensions that may arise between the formal aspects (the procurement process) and the substantive aspects (including specific safeguards in the tender specifications to mitigate the specific risks of procuring an AI solution to meet a public need).

In between, an *ex-ante* AI-impact assessment will empower public purchasers of the NHCS to proactively identify potential risks, such as lack of relevant and representative data, bias, errors, adverse individual or societal impacts, overfitting or underfitting, non-replicable models, black boxes, or lack of transparency, interpretability, and explainability. This assessment will enable the design of appropriate technical and organizational safeguards to be implemented in tender specifications.

While the AIA is still under discussion at the time of writing, some tender specifications are beginning to consider the general alignment of bidders' proposals with the future AIA (Ref. [4], [16]).

Some of the challenges that public purchasers may face when drafting tender specifications can be identified by analysing and characterising the contracts in the sample.

[140] Central Digital and Data Office and Office for Artificial Intelligence (UK), *Assessing if artificial intelligence is the right solution*, 10 June 2019, https://www.gov.uk/.
[141] European Centre for Disease Prevention and Control, *About ECDC, 2024*, https://www.ecdc.europa.eu/; ECDC Public Health Functions Unit, *Call for Tenders OJ/2023/PHF/26497. Artificial intelligence for surveillance and other core public health functions. Framework service contract. Tender Specifications*, 2021/07, version 1.4., https://etendering.ted.europa.eu/.

7.1. *COTS vs bespoke software: tracing CPV Codes and avoiding vendor lock-in risks*

While international or national guidelines on AI procurement do not specify whether public purchases of AI systems should be classified as service or supply contracts,[142] the CPV codification assigned to the contracts in the sample indicates that the procurement of AI software or applications for the NHCS includes both COTS and bespoke solutions, with a clear predominance of the latter. This aligns with the high-demanding technological component of the challenges faced by the NHCS and the specificity of the use cases.

CPV Code	Contract
48460000: Analytical, scientific, mathematical or forecasting software package.	[13]
48180000: Medical software package.	[20]
72000000: IT services: consulting, software development, Internet and support.	[9] [10] [13] [16] [20]
72212180-4: Medical software development services.	[17] [20]
72230000-6: Custom software development service.	[4] [5]
72200000-7: Software programming and consultancy services.	[19]

Table 12. Tracing COTS and bespoke AI software through CPV Codes

However, the same contract may encompass different products and services resulting in a mixed contract. This occurs when an IA COTS solution is purchased, requiring some adaptations, such as incorporating new databases or maintaining and updating the solution. In such cases, the provisions of Article 3 of Directive 2014/24/EU should be considered, and their legal status determined based on the higher estimated value of the respective services or supplies. The practice of EU contracting authorities reveals that many contracts extend beyond the mere acquisition of a COTS or bespoke AI solution. They typically involve other complex ICT products and services[143] including the development of platforms where AI models undergo training, validation, and testing (Refs. [4], [5], [13], [16]-[20]).

The procurement of AI cannot be treated "with the same off-the-shelf purchasing philosophy as other IT systems". First, in the context of public procurement, it is well known that reliance on third-party technology can result in undesirable vendor lock-in effects,[144] especially, in cases of black-box models, reliance on third-party data, non-interoperable AI solutions, restrictive licensing of IPR, or lack of specific provisions in the contract to allow for maintenance of the AI solution independent of the vendors.[145]

Second, the design of public policies legally vested in the authority may be replaced by a "policy making by third party design". In this sense, the decision to optimize a given public task –let's say, clinical triage and validation of medical waiting lists– may involve assumptions about the *expected typical behaviour*, thereby reflecting policy decisions in a manner distinct from other public purchases.[146] Furthermore, as learning from data necessitates making assumptions, different AI models encoded in vendor-

[142] When a software package is procured 'off the shelf' (division 48), it is considered a supply and is governed by the procurement rules on supplies, whereas software programming or the procurement of 'custom software' (division 72) should be considered a service and is governed by the rules on services. See European Commission, *Public Procurement in the European Union. Guide to the Common Procurement Vocabulary (CPV)*, 2008, p. 7. In Spain, the Spanish Central Administrative Court for Contractual Appeals established the following criteria in the in Consultation 58/2018 in relation to the purchase of computer programs. A public contract will be classified as a supply contract when AI solutions already developed and placed on the market are purchased. On the other hand, the contract should be considered as a service contract when the AI solution is customised for the national health system.

[143] For example, in the case of the software and hardware platform to exploit the 'Population Health Database' of the Regional Public Health System of Andalusia (Ref. [13]), the technical specifications covered up to 15 use cases, and the CPV codes of the contract comprised both supplies and services: 72000000-IT Services: consulting, software development, Internet, and support, 32420000-Networking equipment., 48460000-Analytical, scientific, mathematical, or predictive software packages, 48610000-Database systems, 48800000-Information systems and servers, 72212460-Analytical, scientific, mathematical, or predictive software development services, 72312000-Data input services, 72316000-Data analysis services, 72317000-Data storage services, 72322000-Data management services. See Red.es, *Condiciones Específicas del Pliego de Cláusulas Administrativas Particulares que regirán la realización del Contrato de 'Servicio para la implantación de una solución corporativa de analítica avanzada, basada en tecnologías Big data, para el Sistema Sanitario Público de Andalucía'*, PLACE, 4, https://contratacion delestado.es/.

[144] M. Sloane *et al*., *AI and Procurement*, 17.

[145] WEF Guidelines, 26.

[146] *Idem*, 18.

packaged solutions will inevitably make different assumptions, rendering them good for certain tasks but not others.[147]

Third, the so-called "automation-induced complacency"[148] would lead public officials to blindly trust the infallibility of the supplier's AI solution, ultimately resulting in human users routinely relying on the output generated by the solution and not questioning whether it might be flawed (errors in medical software design), unfair (biased health data underrepresenting part of the patient population) or even harmful (false negatives in cancer detection or false positives determining the wrong allocation of public resources).

Finally, public purchasers may be able to buy AI technology as an off-the-shelf product if they are looking for common applications of AI, for example, optical-character recognition. However, buying COTS software may not always be suitable as the specifics of the public-body datasets, the public needs to meet and the problems to solve could mean the supplier would have to build from scratch or significantly customise an existing AI model. In addition, COTS solutions will still need to be integrated into an end-to-end service of the public body,[149] which may envisage satisfying specific and mandatory interoperability and security requirements according to sectoral legislation applicable in the public sector.

An example of vendor lock-in may be the service contract in Ref. [9] for the development, support and maintenance of an advanced expert-healthcare support system. The expert system consisted of a free-text interpretation engine (NLP based on AI), capable of exploiting the clinical information contained in the hospital' EHCR. Previously, in 2016, the hospital had already acquired certain licences for the use of a specific solution that allowed it to exploit the data contained in the medical records. In 2019, the same contractor was again selected through a negotiated procedure without publication for reasons of exclusivity, as the software developer was the only company able to market the platforms previously acquired. In particular, the expert system acquired by the hospital corresponded to the evolution of three modules integrated in of-the-self platforms and then merged into a single application, which was renamed with the registered trademark of the same supplier as in 2016 (Ref. [9]).

7.2. *Gold-plated v. functional specifications*

In general, public buyers can draft technical specifications descriptively (input specification) or functionally (output specification). Whereas a descriptive specification provides a clear framework within which the public purchaser can oversee the contractor's performance, the rigidity of the specifications may leave no room or incentive for innovation or improvement of the good or service. With descriptive specifications, the public buyer prescribes the detailed solution and takes full responsibility for its quality and performance levels. Over-specifying can inflate costs, prompting public buyers to ensure that the 'gold-plated' option aligns with their actual needs.[150]

In addition, there is a high risk of artificially narrowing down competition and favouring specific processes or applications, in breach of Article 42.4 of Directive 2014/24/EU.[151]

Where the purchaser has a good understanding of the market potential or the most suitable technology to meet the public needs, descriptive technical specifications are most useful. However, even in these situations, some flexibility in the performance parameters can facilitate innovation and ultimately contribute to the achievement of the desired outcome.[152]

Conversely, functional specifications establish minimum requirements concerning the methods for achieving a desired outcome and prevent excessively low-performing tenders. EU legislation on public procurement promotes functional and performance specifications, considering them suitable for

[147] Cfr. P. Domingos, *The Master Algorithm. How the Quest for the Ultimate Learning Machine will remake your World*, New York, Basic Books, 2018, 24.
[148] R. Binns and V. Gallo, *Automated Decision Making: the Role of Meaningful Human Reviews*, Information Commissioner's Office [UK], 12 April 2019, https://ico.org.uk.
[149] Office for Artificial Intelligence and Government for Digital Service, *A guide to using artificial intelligence in the public sector*, 27 January 2020, 16, https://www.gov.uk/.
[150] Crown Commercial Service, *How to write a specification –Procurement Essentials*, 16 November 2021, www.crowncommercial.gov.uk.
[151] Cfr. Recital (74) Directive 2014/24/EU.
[152] C(2021) 4320 final, 42-43.

fostering innovation.[153]

Most of the tender specifications in the sample do not prescribe a particular AI solution but rather make a general reference to AI strategies to achieve the desired outcomes (Ref. [4], [9], [10], [11], [13], [14], [15], [16], [17], [18], [19]) mostly enunciated as use cases. At times, AI may not be the sole approach, and the contract leaves room for other data-driven technologies, such as blockchain (Ref. [15]). In some cases, the specifications detail the AI strategy and the learning models to be developed by the contractor (Refs. [3], [5], [8], [12]).[154]

For example, the tender launched by the European Centre for Disease Prevention and Control sought the implementation of AI, including ML and DL, in the processes and tasks related to surveillance and other core public-health functions, as well as the related training required to properly handle and sustain these outputs (Ref. [3]). In this respect, the tender specifications described in a general way the strategies, the learning problem and the models to be implemented according to the instructions given in the corresponding deliverables (DLV).

Strategy, learning problem and models for disease prevention and control	
DLV 5	**ML model for regression or classification**
	The objective is to prepare a ML model to solve a regression problem using K nearest neighbours (K-NN), linear regression, linear support vector machine (SVM) or similar methods; or to solve a classification problem using k-NN, logistic regression, decision trees, random forest, linear or Radial basis function SVM, or similar methods.
DLV 6	**DL model for regression or classification problem**
	The objective is to prepare a DL model to solve a regression or classification problem using neural networks, convolutional neural networks or similar methods.
DLV 7	**Unsupervised model**
	The objective is to prepare a ML/DL unsupervised model on clustering for anomaly detection, data/image clustering, segmentation, among others; or on dimensionality reduction for data compression, noise reduction and data visualisation, among others.

Table 13. AI strategy, learning problems and models in tender specifications

Functional specifications are used to identify the essential properties of AI models to ensure their quality and trustworthiness (e.g., accuracy, performance, transparency, interpretability, or explainability). These properties can be described in tender specifications as general goals for the contractor to achieve, rather than imposing specific thresholds. This is evident in the technical specifications of the Population Health Database project (Ref. [13]).[155]

Safeguards to ensure trustworthiness of AI models
Analytical Modelling - Selection of the analytical-modelling approach: the most appropriate analytical-modelling technique(s) will be selected for each use case based on the problem to be solved. - Evaluation design: prior to constructing the analytical model, the evaluation method to be employed to determine the quality and validity of the analytical model (based on parameters such as its performance, reliability, robustness, or explainability, among others) will be defined and approved by Red.es. - Model construction and training: once the analytical-modelling technique(s) has(have) been selected, the model will be constructed and trained on the previously-prepared data. One or more analytical models may be generated in this phase. - Evaluation of the analytical model: the analytical models will be interpreted based on pre-existing knowledge and pre-established success criteria. In this evaluation phase, factors such as accuracy and generality of the model will be assessed.

Table 14. Example of functional specifications

In the same vein, tender specifications sometimes require the contractor to ensure the accuracy of the models by implementing various metrics, but without defining the specific metric or establishing concrete

[153] Recital (74) and 42(3) (a) of the Directive 2014/24/EU.

[154] In relation to ML strategies or paradigms, learning problems and frequent models, see European Union Agency for Cibersecurity (ENISA), *Securing Machine Learning Algorithms*, December 2021, 7-10, DOI: 10.2824/874249.

[155] See Red.es, *Pliego de Prescripciones Técnicas*, 50.

thresholds. For example, in relation to the expert system tendered by the Government of Valencia to assist 112 operators in classifying healthcare needs for hospital and out-of-hospital emergencies, the technical specifications require an evaluation of the system on the basis of "different metrics" from the point of view of its clinical, economic and social impact (Ref. [8]). Similarly, the two calls for tenders launched by the Galizia Health Service (SERGAS) for the development of a personal assistant system (AVATAR) to increase patient autonomy (Ref. [10]) and the support system for cancer detection based on image analysis using AI (Ref. [11]) included, as one of the award criteria, "the level of detail of the proposed indicators and *metrics* to be used to verify the achievement of the proposed functional objectives (emphasis added)".

7.3. *Appropriate definitions*

The standard clauses provided by the tender specifications should include a list of appropriate and specific definitions in relation to the subject-matter of the public contract and the context of development and implementation of the AI solution that will be procured.

Providing appropriate definitions in the tender specifications can be quite challenging as many AI-related concepts may have different meanings depending on the context and the relevant stakeholders involved. Therefore, the substantiation of the relevant concepts in the tender specifications could be necessary.

A typical example of this could be the term "(algorithmic) transparency". Depending on the relevant domain concerned, "transparency" may have different meanings, namely the technical domain (e.g., in the field of 'XAI'), the ethical domain (e.g., OECD Recommendations, EU HLEG Guidelines, Alan Turing FAST Truck Principles), the legal domain (Article 13 of the AIA) and the contractual domain (WEF Guidelines, EU Commission Standard Clauses, Amsterdam Standard Clauses, Barcelona Methodologies). In addition, the degree of algorithmic transparency required in a particular context may require timely and appropriate adaptation of the relevant information on the AI system in relation to the affected stakeholders. These stakeholders may include the public purchaser and public employees as end-users of the AI system, supervisory authorities, individuals and groups likely or intended to be affected by the AI system, or even citizens as legitimate holders of freedom of information rights.

Another polysemic term is "parameter". For example, in ML contexts a "parameter" is an internal variable of the model that affects how it computes its outputs. Parameters are tuned during the training of the model using some optimisation procedures.[156] Although the AIA refers to the term 'parameter' in this proper technical meaning,[157] it is important to note that the term is often used by the lawmaker as a blanket concept, the exact meaning of which remains undefined.[158]

A list of AI-related definitions is included in the standard clauses of both the EU Commission and the City of Amsterdam.

European Commission	City of Amsterdam
AI System	Algorithmic System
Intended Purpose	Intended Use
Public Organisations Datasets	Decisions
Supplier Data Sets	Procedural

[156] See, for instance, ISO/IEC 22989:2022(en). Information technology - Artificial intelligence - Artificial intelligence concepts and terminology, at 3.3.4 and 3.3.8. Examples of parameters are "coefficients" of linear and logistic regression models, "weights" and "biases" in a neural network. Unlike parameters, the "hyperparameters" are values which control the learning process and the model parameters resulting from it. Hyperparameters are selected prior to training and can be used in the processes to help estimate model parameters. Examples of hyperparameters include the number of network layers, learning rate for neural networks; the number of leaves or depth of a tree; K value for K-means clustering or the maximum number of iterations of the expectation maximization algorithm.

[157] See Article 3(29) in relation to the training model and Annex IV.2.b) in relation to the technical information of the AI system to be provided to end-user, inter alia, "the relevance of the different parameters" within the system.

[158] For example, Article R.311-3-1-2 of the French the Code of Relations between the Public and the Administration (CRPA) specifically stipulates that the individual administrative decisions shall contain a notice informing, among other aspects, about "the *processing parameters*, and, where appropriate, their weighting, applied to the individual situation of the interested party". The Spanish Law 12/2021, on 28 September has amended the Employees Statute of 2015 in order to recognise the right of the works council to be informed by the company of "the *parameters*, rules and instructions on which algorithms or artificial intelligence systems are based, that affect the decision-making having an impact on working conditions, access to and maintenance of employment, including profiling".

and Third-Party Data Sets	Transparency
Reasonably Foreseeable Misuse	Technical Transparency
Substantial Modification	Explainable/ Explainability

Table 15. Definitions in tender specifications

Unlike the European Commission Standard Clauses, the City of Amsterdam defines "Algorithmic System" instead of "AI System". The reason for this option is twofold. Firstly, it was opted to bring applications using data analysis and/or statistics and other elements of the definition within the scope of the Standard Clauses. This is because, in actual practice, certain software often employed lacks self-learning logic (or any other AI strategy), but its application can still have significant, and sometimes unforeseen or unintended, impacts on citizens. Secondly, the term "Algorithmic System" is more aligned with the principle of technological neutrality, as it ensures the applicability of the Standard Clauses "on the basis of the impact the algorithmic system has on CITIZENS rather than on the basis of the technology used",[159] whether or not it is AI-enabled technology.

This point is crucial because some algorithmic systems implemented by public administrations have been questioned by supervisory authorities or courts precisely due to their adverse impacts on the rights and interests of the governed.[160] Therefore, the algorithmic systems within the scope of the Amsterdam Standard Clauses make it possible that certain safeguards will be applicable to them, such as requirements to ensure statistical inaccuracy, fairness and explicability of outcomes. Also, it is noteworthy that the AIA also encompasses "statistical approaches" in the list of AI techniques and approaches. In this regard, the Canadian Directive on Automated Decision-Making of 2019 applies to automated decision systems that "draw from fields like statistics".

7.4. *The "intended purpose" of the AI system: describing the problem*

The "intended purpose" or "intended use" describes the specific problem or problems previously identified by the public purchaser and that the AI/algorithmic system is to solve. In this context, the term "problem" should be interpreted in a broad sense.[161]

Public purchasers should be clear about the "intended use" of the AI/algorithmic solution, specifying "what exactly it can be used for and the exact conditions under which it can be used". In addition, a clear determination of the "intended use" is also relevant to assess the solution's performance, especially in self-learning models.[162]

An example of a description of the "intended purpose" of an AI system is the AZUD project (Ref. [14]), led by the Health Service of the Autonomous Community of Murcia ("SMS"). This project sought to develop and implement a data-lake platform that would allow the storage of any type of useful information, supporting a big data approach oriented towards clinical practice with patients. An important part of the information systems of the SMS is devoted to the analysis of previously collected data in order to obtain relevant information for healthcare management and decision-making at different organisational levels. This healthcare and administrative information is stored in a data warehouse in a structured format. On the basis of this existing infrastructure, the SMS then considered the need to capture and process the large amount of patient-generated information which is available in the existing systems (internal and external). In the memorandum justifying the public need to be met by the performance of the contract, the SMS described the challenge and the problems to be solved by the contractor.[163]

[159] See Amsterdam Standard Clauses, 5-6.

[160] This is the case of some algorithmic systems applied in the education sector to assign vacant positions to teaching staff according to the interprovincial mobility call (such as the algorithm of the Ministero dell'Istruzione, dell'Università e della Ricerca in Italy), to automatically process the national pre-enrolment procedure in the first year of public university (like Parcoursoup in France), to predict the grade that students would have achieved if official exams had taken place (as implemented by Ofqual in the United Kingdom). See M.E. Gutiérrez David, *Government by Algorithms at the Light of Freedom of Information Regimes. A Case-by-Case Approach on Automated Decision-Making Systems within Public Education Sector* in *Indiana Journal of Global Legal Studies*, vol. 30, no. 2, 2023, 105-172.

[161] Amsterdam Standard Clauses, 7.

[162] UK NHS Buyer's Guide, 10, 25.

[163] Servicio Murciano de Salud, *Memoria de Necesidad e Informe de Propuesta. Data Lake Sanitario del Servicio Murciano de Salud Proyecto "AZUD"*, Subdirección General de Tecnologías de la Información, 28 May 2021, 3-4, https://contrataciondelestado.es/.

SMS' AZUD PROJECT
The large amount of clinical information and the variety of formats and sources of information (external and internal) useful for clinical practice represent a technological challenge that can only be met by employing new storage, processing and analysis mechanisms. In order to transform this amount of patient information into useful insights for clinical practice, it is necessary to: 1. Facilitate the integration of internal-information sources (first-party data), information sources from collaborating companies and organisations (second-party data), and third-party information sources (third-party data). 2. Industrialise the complex data processes through automatic orchestration. 3. Correlate these disparate sources for informed clinical decision-making that is not currently available. 4. Define and implement predictive models using machine learning to anticipate anomalous and risky situations and take the necessary action to eliminate or reduce the impact. 5. Industrialise the predictive models to ensure their correct operation over time. 6. Automate the actions triggered by the implemented predictive models.

Table 16. Defining the intended purpose of the AI solution for healthcare

7.5. *Data quality and data governance*

Data, whether personal or not, play a crucial role in the implementation of AI solutions. The importance of this is highlighted in the existing Guidelines for AI procurement, where it is emphasized that clarifying the technical and ethical limitations of data usage in tender specifications is essential. This clarification is necessary to mitigate risks such as bias, discrimination, fairness concerns, unintended individual and societal impacts, or deviation from the intended purpose of the AI system.

Risks in medicine and healthcare encompass various facets, including the potential for AI errors to put patients at risk, privacy and security concerns, and the use of AI in ways that could exacerbate social and health inequalities. This exacerbation can occur either through the incorporation of existing human biases and discriminatory patterns into automated algorithms, or through the use of AI in ways that accentuate disparities in access to healthcare services. Scholars have provided illustrative examples, such as the harm resulting from incomplete or biased data used in the development of an AI-powered pulse oximeter. Due to incomplete data representation, the device tended to overestimate blood oxygen levels in patients with darker skin, leading to undertreatment of their hypoxia.[164] In the same way, racial biases have been reported in algorithms of healthcare programmes for high-risk patients in COTS solutions procured by public-health systems.[165]

In particular, there is scientific evidence that race-adjusted algorithms are being employed in clinical practices, perpetuating health inequities. Scholars have compiled some of these algorithms that incorporate race correction. Adjustments in AI models are typically justified on the basis of the existing patterns extracted from historical data and concerning patient attributes, clinical outcomes, and certain assumptions about what is considered the *ground truth*.[166]

Relevant studies have indicated that many AI applications designed for diagnosing

[164] F. Federspiel, R. Mitchell, A. Asokan, C. Umana and D. McCoy, *Threats by artificial intelligence to human health and human existence*, in *BMJ Specialist Journals*, vol. 8, no. 5: e010435, 2023, DOI: 10.1136/bmjgh-2022-010435.

[165] Z. Obermeyer, B. Powers, C. Vogeli and S. Mullainathan, *Dissecting racial bias in an algorithm used to manage the health of populations* in *Science*, no. 366 (6464), 2019, 447-453, DOI: 10.1126/science.aax2342.

[166] D. A. Vyas, L. G. Eisenstein and D. S. Jones, *Hidden in Plain Sight - Reconsidering the Use of Race Correction in Clinical Algorithms*, in *The New England Journal of Medicine*, vol. 383, 2020, 874-882, https://www.nejm.org/doi/10.1056/NEJMms2004740. The authors have analysed the use of algorithmic models in several areas of clinical practice (e.g. cardiology, obstetrics, nephrology, and urology). The research illustrates some significant examples. Because of the difficulties in measuring kidney function directly, some algorithmic models have been developed to determine the estimated glomerular filtration rate (eGFR) from a measurable indicator such as the serum creatinine level. Higher eGFR values indicate better kidney function. The algorithmic models tend to report higher eGFR values for black people. This is based on the idea that black people release more creatinine into the blood, partly because they are supposed to be more muscular. Analyses have questioned this assumption, provided that "race is a social rather than a biological construct". In despite of this, the race-corrected eGFR still remains the standard. It is argued that discarding race adjustment of eGFR could lead to overdiagnosis or overtreatment of black individuals, even if such adjustment could delay referral of these patients for specialist care or transplantation.

COVID cases or predicting patient outcomes - some of which are commercialised and utilized in hospitals - were deemed unsuitable for clinical use due to serious errors in the data they relied upon, posing a high risk of bias.[167]

Taking into account the existing Guidelines for IA procurement, public purchasers of the NCHS should consider the following circumstances when drafting tender specifications:[168]

1. appropriate analysis (collection, when necessary), structuring and editing of data according to a motivated approach in relation to the specific domain of application or use cases;
2. whether all data to be included in the databases have the same level of protection;
3. whether the data meet the criteria of fairness and avoidance of bias;
4. the possible limitations (due to representativeness, provenance, clarity, completeness, accuracy, proxy predictors) of the data should be assessed in advance;
5. appropriate data-governance schemes and personal-data protection.

In the first place, large quantity of data is required to develop AI solutions, specially, in the context of personalised medicine and other potential high-risk applications of AI in the domain of healthcare. In this regard, public purchasers should assess whether their data are of high-enough quality for AI, considering the following elements: accuracy, completeness, uniqueness, timeliness, validity, sufficiency, relevancy, representativeness, and consistency.[169]

In the second place, considering that most of the tenders in the sample require the implementation of ML or DL approaches, the quality of data becomes of paramount importance due to the strong ties between quality and accuracy of AI models. In effect, when assessing the accuracy of learning methods using public-health datasets of an observational nature, or surveys with high non-response rates, it is crucial to consider the presence of bias within the dataset. Bias occurs when the dataset does not accurately represent the population of interest in significant aspects. This mismatch may result in accuracy estimates that cannot be reliably replicated when these methods are implemented in real-world scenarios. Another issue to bear in mind is the presence of confounders, i.e. variables that are correlated with both the outcome and the predictors. AI models may inadvertently learn to predict these confounding variables rather than the actual outcome of interest, leading to inflated accuracy within the dataset. Furthermore, when bias and confounding variables co-exist, the situation becomes even more problematic. In such cases, confounding variables may be correlated with the outcome within the dataset, but not within the broader population. This scenario may result in a learning model that appears to be highly accurate within the dataset, but is ultimately ineffective for practical purposes.[170]

In the third place, the data quality of training, validation and testing-data sets is a pivotal requirement of the AIA.[171]

[167] See The Alan Turing Institute, *Data science and AI in the age of COVID-19. Reflections on the response of the UK's data science and AI community to the COVID-19 pandemic*, 13-14, 2021, www.turing.ac.uk; L. Wynants, B. Van Calster, G. S Collins *et al*. *Prediction models for diagnosis and prognosis of covid-19: systematic review and critical appraisal* in *BMJ* (Clinical research ed.), vol. 369, m.1328, 7 April 2020, Doi: 10.1136/bmj.m1328; M. Roberts, D. Driggs *et al.*, *Common pitfalls and recommendations for using machine learning to detect and prognosticate for COVID-19 using chest radiographs and CT scans* in *Nature Machine Intelligence*, vol. 3, 2021, 199-217, https://doi.org/10.1038/s42256-021-00307-0; W.D. Heaven, *Hundreds of AI tools have been built to catch covid. None of them helped* in *MIT Technology Review*, 30 June 2021, www.technologyreview.com. Common errors detected encompassed the utilization of poor-quality data due to incorrect labelling, the inclusion of duplicate data, sourcing data from unknown origins, incorporating data that did not accurately represent the target population (such as paediatric patients), or the underrepresentation of vulnerable and underserved groups (such as ethnic minorities or low socio-economic status populations). Furthermore, inadequate or absent internal or external validation of models, along with overfitted models –trained on insufficient or small datasets, were also identified. Consequently, the predictive performance of some tools might have significantly diminished in real clinical settings when confronted with new input data.

[168] WEF Guidelines, 18-19; NHSX A Buyer's Guide, 14, 44, 51; Amsterdam Standard Clauses, 14; Barcelona Methodologies, 15-16, 18.

[169] WEF Guidelines, 7; Central Digital and Data Office and Office for Artificial Intelligence, *Guidance Assessing if artificial intelligence is the right solution*, 10 June 2019, https://www.gov.uk/.

[170] D. Pigoli, K. Baker, J. Budd *et al*., *Statistical Design and Analysis for Robust Machine Learning: A Case Study from COVID-19*, arXiv:2212.08571v2 [cs.SD], 27 February 2023, https://arxiv.org.

[171] See Recital (44) of the AIA: "High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models

In this sense, Article 10 of the AIA subjects these data sets to appropriate data-governance and management practices. In line with such practices, tender specifications should consider: the relevant design choices; data collection (making a clear a clear distinction between healthcare data provided by public purchaser, the contractor or third-parties); relevant data preparation processing operations (e.g., annotation, labelling, cleaning, enrichment, aggregation); the formulation of relevant assumptions, notably with respect to the information that the data are supposed to measure and represent; a prior assessment of the availability, quantity and suitability of the data sets that are needed to design the AI solution for the intended purposes; examination in view of possible biases; the identification of any possible data gaps or shortcomings, and how those gaps and shortcomings can be addressed; trainings' relevant representativeness, completeness and freedom from errors , data sets' validation and testing, including adequate statistical properties as regards the persons or groups of persons (e.g., clinicians, patients, caregivers, targeted population) on which the AI system is intended to be used; the intended purpose of the AI system in relation to the features or elements that are peculiar to the specific geographical, behavioural or functional setting within which the AI system is intended to be used.[172]

The European Commission emphasizes that for non-high-risk AI, compliance with data quality and other requirements[173] is not mandatory under the AI Act. Nonetheless, the Commission suggests that contractual clauses for the procurement of AI by public purchasers enhance the reliability of AI applications acquired by public organizations. This can be achieved by incorporating specific contractual provisions tailored to non-high-risk AI systems.[174]

When looking at the tenders of interest, tender specifications do include specific provisions on data pre-processing (Ref. [3], [4], [19]), data governance ([2], [4], [18], [20]) or training, validation or testing of models and re-training with new data.

Typically, data-quality requirements are formulated in a very general and broad manner. Technical specifications provided by the Regional Health Service in Murcia have established a number of requirements in relation to data quality.[175]

Data quality requirements in the AZUD Project
Data quality: Tools are necessary to measure and display the quality of data stored in the Data Lake, with the following objectives: Providing contextual information about the datasets (metadata). Identifying distinct dimensions using a unique ID. Mapping and standardising information where feasible. Establishing key performance indicators (KPIs) to identify potentially erroneous data.

Table 17. Data quality requirements in tender specifications

Some tender specifications require appropriate safeguards to ensure the replicability of the AI models developed (Ref. **[2]**). The joint procurement launched by the European Food Safety Authority (EFSA) and other EU bodies defined the following data-management tasks.[176]

Data management tasks in epidemiological analyses
Data management tasks may include data analysis (including related data management when necessary), statistical or mathematical modelling, simulation modelling, design and analysis of the results of epidemiological

are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by Union law. High quality training, validation and testing data sets require the implementation of appropriate data governance and management practices".

[172] See Article 10(2), (3), and (4) of the AIA; Article 3 of the European Commission Standard Clauses.

[173] The European Commission Standard Clauses encompass mandatory requirements under the AIA such as technical documentation, risk management system, automatic recording of events (logging capabilities), transparency, human oversight, accuracy, robustness, cybersecurity, quality management system, conformity assessment, corrective actions, post-market monitoring.

[174] European Commission, *Proposal for standard contractual clauses for the procurement of artificial intelligence by public organisations version*, 4 April 2023, https://public-buyers-community.ec.europa.eu/.

[175] Servicio Murciano de Salud, *Pliego de Prescripciones Técnicas. Data Lake sanitario del Servicio Murciano de Salud Proyecto "AZUD"*, Subdirección General de Tecnologías de la Información, 28 May 2021, 7, https://contrataciondelestado.es/.

[176] EFSA, *Updated Tender Specifications. Assistance for Statistical and Epidemiological Analyses and related data management, using conventional and Artificial Intelligence methodology, and for training and ad hoc consultation upon request*, 16 October 2020, 7, https://etendering.ted.europa.eu.

studies, computational support, and methodological consultations or training. This may require the processing and loading of data in various formats (e.g. structured text files, SAS datasets, Excel spreadsheets, XML, MS Access and Oracle Databases) and the use of specific software (e.g. R, STAN, SAS, Python etc.). Additionally, the contractor should be able to provide Artificial Intelligence (AI)/Machine Learning (ML) solutions in case they can be considered appropriate/relevant or an improved way of dealing with the problems at hand. Each task will require appropriate reporting and documentation to allow reproducibility of all results.

Table 18. Replicability of AI models

In the tender specifications corresponding to the call for tender launched by the Catalan Institute of Health, te team of Data Scientists from the successful bidder were tasked with developing and training predictive algorithms on the Cloudera Corporate Platform supporting clinical decision making in the integral care of critical patients. Specific tasks were needed to ensure data quality.[177]

Preparing data sets and AI models for Health Data Lakes infrastructures
- Processing, cleaning, normalizing, and harmonizing historical data from the Data Lake within the Cloudera Corporate Cloud Platform. - Implementing methods to correct missing or erroneous data wherever feasible. - Conducting exploratory data analysis in collaboration with clinical professionals to gain insights. - Recommending a set of the most suitable Machine Learning or Deep Learning algorithms and providing training. - Evaluating and validating the optimal model based on quality criteria defined by CatSalut. - Conducting on-demand re-training of the model using new data from patients who have completed their ICU stay.

Table 19. Pre-processing of health data, training, validating and testing AI models

[177] Institut Catàla de la Salut, *Plec de prescripcions tècniques per a la contractació de l'entorn d'intel·ligència artifical i uci estesa del projecte de millora i ajuda a la presa de decisions clíniques de l'atenció integral del pacient crític en l'Hospital Universitari de Bellvitge i el Consorci Corporació Sanitaria Parc Taulí*, 29 July 2022, 8, https://contractaciopublica.cat.

7.6. *Transparency and explainability of the AI system*

Requirements for "interpretability", "transparency", and "explainability" of AI systems are commonly found in the wording of soft law and sectoral legislation on AI. Often, these terms are used interchangeably. However, in the technical domain, these concepts have distinct meanings. Specifically, in the field of Explainable Artificial Intelligence (XAI), there is a distinction between them.[178]

[178] Firstly, the "interpretability" means how understandable or intelligible an AI model is to a human observer. The interpretability of a model is greater if it is easy for a person to reason and trace in a coherent way why the model arrived to a particular decision or outcome. See A. Barredo *et al.*, *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible* AI, in *Information Fusion*, vol. 58, 2020, 82, 84. https://doi.org/10.1016/j.inffus.2019.12.012; D. V. Carvalho, E. M. Pereira, J. S. Cardoso, *Machine Learning Interpretability: A Survey on Methods and Metrics*, in *Electronics*, vol. 8, no. 8, 832, 2019, https://doi.org/10.3390/electronics8080832.
Secondly, the "transparency" of an AI model is determined by the degree of intrinsic interpretability of a specific model. Therefore, transparency is an attribute of the model that defines the degree of comprehensibility that a model itself has for a human observer. Transparency can be assessed at three levels. Firstly, at the model level ("simulability"), it involves how replicable the model is by a human from its data and parameters in a reasonable time. Secondly, at the component level ("decomposability"), it involves the intuitive explanation of the model's components, including inputs, parameters. Thirdly, concerning the learning algorithm ("algorithmic transparency"), it refers to understanding the process that the model employs to generate a specific outcome from the data. See B. Mittelstadt, C. Russell and S. Wachter, *Explaining Explanations in AI*, in *Proceedings of the Conference on Fairness, Accountability, and Transparency*, FAT* '19, January 2019, 2. http://dx.doi.org/10.1145/3287560.3287574; B. Lepri, N. Oliver, E. Letouzé *et al*., *Fair, transparent and accountable algorithmic decision-making processes. The premise, the proposed solutions, and the open challenges* in *Philosophy & Technology*, vol. 31, 2018, 611, 619; ICO & Alan Turing Institute, *Explaining decisions made with AI*, last update 27 October 2022, 69, https://ico.org.uk/. Consequently, an AI model is considered transparent if it is interpretable by itself (i.e., if the overall performance of the model, its individual components, and its learning algorithm are intelligible or understandable to a human). See Barredo, *Explainable Artificial Intelligence*, 88–100.
Finally, the "explainability" is an active attribute of the model that refers to the ability to generate an explanation of the model's behaviour based on the data used, the results obtained, and the entire decision-making process according to the audience for which the explanation is intended (e.g., authorities, experts, third-party auditors, certification bodies, public at large, individuals affected by the model's decision). Explanations are instruments by which the decisions of an AI model can be

In relation to AI solutions for NHCS qualified as high-risk, the AIA would impose transparency obligations (Article 13): "High-risk AI systems shall be designed and developed in such a way to ensure that their operation is *sufficiently transparent* to enable users to interpret the system's output and use it appropriately. An *appropriate type and degree of transparency* shall be ensured, with a view to achieve compliance with the relevant obligations of the user and of the provider set out in Chapter 3 of this Title [emphasis added]".[179]

However, the approach taken by the AIA appears insufficient.[180]

Firstly, the European Commission's proposal lacks legal definitions for key terms such as "transparency", "sufficiently transparent", "to interpret" or "explainability". Consequently, the responsibility for making AI systems interpretable and explainable falls within the discretion of the AI system provider or developer.

Secondly, the appropriate form and level of transparency appear to be relative and merely instrumental with a view to achieve compliance with other requirements of the AIA, as emphasized in Recital 47, which calls for "a degree of transparency". The broad wording of the AIA could imply that a general form of transparency, provided through "relevant documentation" and "instructions", may satisfy this requirement by covering aspects like the intended purpose, accuracy, robustness, risks, performance metrics, input-data specifications, *inter alia*.

Thirdly, the AIA does not address the concept of "explainability", so it remains open to interpretation the question of whether Article 13 of the AIA requires the implementation of XAI techniques (e.g., subrogate models, LIME, SHAP, counterfactuals) and the choice of approach (e.g., post-hoc, local or global explanations) to ensure interpretable models.

Furthermore, the Commission's approach to explainability represents a significant departure from that proposed by the HLEG Ethics Guidelines. In the AIA, explainability remains completely blurred, with Recital (47) being the sole explicit reference to it within the entire Commission's proposal.[181] By contrast, explainability is a core element of ethical and trustworthy systems within the HLEG Guidelines, as it is addressed not only

explained in a more clear, understandable, transparent, and interpretable manner. Therefore, if interpretability is the ultimate goal, explanations are tools to achieve the interpretability of the model. Carvalho, *Machine Learning*, 15. In turn, a distinction must be made between models that are "interpretable by design" (i.e., "transparent models") and models that, not being interpretable *prima facie*, can nevertheless be explained by means of different techniques which extract relevant information from the model to generate explanations. Mittelstadt *et al.*, *Explaining Explanations*, 83.

[179] Pursuant to Articles 13(2) and (3), high-risk AI systems shall be accompanied by instructions for use that shall include concise, complete, correct, clear, relevant, accessible and comprehensible information to users. The information shall include: characteristics, capabilities and limitations of performance of the high-risk AI system (intended purpose, the level of accuracy, robustness and cybersecurity tested and validated, any known or foreseeable circumstance which may lead to risks to the health and safety or fundamental rights, its performance as regards the persons or groups of persons affected by the system, specifications for the input data, or any other relevant information on the training, validation and testing datasets used); the changes to the high-risk AI system and its performance pre-determined by the provider at the moment of the initial conformity assessment; the human oversight measures; the expected lifetime of the high-risk AI system and any necessary maintenance and care measures.

[180] See D. Schneeberger, R. Röttger, F. Cabitza *et al.*, *The Tower of Babel in Explainable Artificial Intelligence (XAI)*, in A. Holzinger, P. Kieseberg, F. Cabitza *et al.* (eds.), *Machine Learning and Knowledge Extraction. CD-MAKE 2023. Lecture Notes in Computer Science*, vol 14065, Cham, Springer, 2023, 65, 70. https://doi.org/10.1007/978-3-031-40837-3_5.

[181] Recital (47) of the AIA reads as follows: "Furthermore, the exercise of important procedural fundamental rights, such as the right to an effective remedy and to a fair trial as well as the right of defence and the presumption of innocence, could be hampered, in particular, where such AI systems are not sufficiently transparent, *explainable* and documented [emphasis added]." If, from a technical standpoint, explanations are tools to achieve the interpretability of non-transparent models, then it could be argued that XAI techniques to ensure explainability may be implied by Article 13(3)(d) of the AIA. This provision requires that instructions accompanying the high-risk system shall include "the human oversight measures referred to in Article 14, including the *technical measures put in place to facilitate the interpretation of the outputs of AI systems by the users* [emphasis added]. In particular, Article 14(4)(d) mandates that technical measures to ensure human oversight shall allow to "*correctly interpret* the high-risk AI system's output, taking into account in particular the characteristics of the system and the *interpretation tools and methods available*." Annex IV (d) reiterates the need to include this information in the technical documentation. Regardless of the intended meaning behind the aforementioned provisions, the fact is that the AIA presents two significant shortcomings: the absence of requirements regarding the model explainability and the apparent oblivion –deliberate or not– in relation to concrete guarantees of transparency and explainability for potential recipients of algorithmic systems, whether individuals, specific groups, or society at large.

to the user of the system, but also to the collectives and individuals affected by the decisions or outcomes of the system.[182]

The European Parliament introduced an amendment in Article 13(1) defining transparency.[183] Accordingly, the Parliament included a new Article 68(c), which recognised the right to an explanation of individual decision-making, clearly echoing Recital (71) of the GDPR. This right would be enforceable where a decision or output of high-risk systems produce legal effects, or similarly significantly affect a person in a way that he or she considers to adversely impair his or her health.[184] The Draft Agreement also recognises this right to an explanation, with some relevant changes to the Parliament's version.[185]

The constraints identified in the AIA could lead to a downgrading of the level of guarantees required in the public procurement of AI solutions in healthcare.

Against this background, the Amsterdam Standard Clauses differentiates between "Procedural Transparency",[186] "Technical Transparency"[187] and "Explainability",[188]

[182] The HLEG Ethics Guidelines, at 18, defines the explainability as "the ability to explain both the technical processes of an AI system and the related human decisions (e.g. application areas of a system)." The Guidelines make a difference between *ad-intra* explainability (technical explainability), and *ad-extra* explainability (collective or individuals concerned). "Technical explainability – explains the HLEG– requires that the decisions made by an AI system can be understood and traced by human beings. Moreover, trade-offs might have to be made between enhancing a system's explainability (which may reduce its accuracy) or increasing its accuracy (at the cost of explainability). Whenever an AI system has a significant impact on people's lives, it should be possible to *demand a suitable explanation of the AI system's decision-making process*. Such explanation should be timely and adapted to the expertise of the stakeholder concerned (e.g. *layperson*, regulator or researcher). In addition, explanations of the degree to which an AI system influences and shapes the organisational decision-making process, design choices of the system, and the rationale for deploying it, should be available".

[183] The new sub-paragraph in Article 13(1) reads: "Transparency shall thereby mean that, at the time the high-risk AI system is placed on the market, all technical means available in accordance with the generally acknowledged state of art are used to ensure that the AI system's output is interpretable by the provider and the user. The user shall be enabled to understand and use the AI system appropriately by generally knowing how the AI system works and what data it processes, *allowing the user to explain the decisions taken by the AI system to the affected person* pursuant to Article 68(c) [emphasis added]". This provision has been removed from the Draft Agreement reached by the co-legislators in January 2024, and has instead been included in Recital (14a).

[184] The provision introduced by the Parliament stipulated that: "1. *Any affected person* subject to a decision which is taken by the deployer on the basis of the output from a high-risk AI system which produces legal effects or similarly significantly affects him or her in a way that they consider to adversely impact their health, safety, fundamental rights, socio-economic well-being or any other of the rights deriving from the obligations laid down in this Regulation, shall have *the right to request from the deployer clear and meaningful explanation* pursuant to Article 13(1) on the role of the AI system in the decision-making procedure, the main parameters of the decision taken and the related input data. 2. Paragraph 1 shall not apply to the use of AI systems for which exceptions from, or restrictions to, the obligation under paragraph 1 follow from Union or national law are provided in so far as such exception or restrictions respect the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society. 3. This Article shall apply without prejudice to Articles 13, 14, 15, and 22 of the Regulation 2016/679 [emphasis added]."

[185] Compare the European Parliament's version of Article 68(c) with the version proposed in the Draft Agreement. Whereas the former recognised "the right to request from the provider a clear and meaningful explanation, in accordance with Article 13(1), of the role of the AI system in the decision-making process, the main parameters of the decision taken and the related input data"; the Draft Agreement eliminates the reference to Article 13(1) and opens the door for the user of the high-risk system to freely determine "the main elements of the decision taken". Furthermore, Article 68(c)(2) of the Draft Agreement has removed safeguards against any restriction or derogation to this right in the Union or Member State legislation by suppressing the requirement that the exceptions or limitations must "respect the essence of fundamental rights and freedoms and [be] a necessary and proportionate measure in a democratic society".

[186] See Amsterdam Standard Clauses, 8. "Procedural Transparency" is defined as "the provision of information on the purpose of the Algorithmic System and the process followed in the development and application of the Algorithmic System and the data used in that context, which should in any event be deemed to include the provision of an understanding of the choices and assumptions made, the categories of data used in the development of the Algorithmic System, the way in which human intervention is provided for in the Algorithmic System, the method used to identify risks, the risks identified, and the measures taken to mitigate the risks, as well as the parties that were involved in the development of the Algorithmic System and their roles."

[187] See Amsterdam Standard Clauses, 9 "Technical Transparency" is defined as "the provision of information enabling [the contracting authority] to understand the technical operation of the Algorithmic System, which may in any event be deemed to include the disclosure of the source code of the Algorithmic System, the technical specifications used in developing the Algorithmic System, the data used in developing the Algorithmic System, technical information on how the data used in developing the Algorithmic System were obtained and edited, information on the method of development used and the development process undertaken, substantiation of the choice for a particular model and

indicating a clear alignment with the HLEG Ethical Guidelines.

By ensuring Procedural Transparency, the contracting authority should seek to:[189]

- Gain an understanding of the process followed by the contractor in the development and application of the system and the choices made by the contractor during that process.
- Form an opinion on the quality of an algorithmic system without needing the information that is required if Technical Transparency is to be provided.
- Be able to provide general information to citizens or individuals affected on the use of the system and to explain the operation thereof, thus ensuring accountability.

By including Technical Transparency clauses, the contracting authority seeks to gain all the information that is necessary to assess the technical quality and the technical operation of the system, including the disclosure of the source code, the technical specifications used in developing the system, and appropriate information on the data used in developing the system (how the data were obtained, edited and used), the substantiation of the choice for a particular model and its learning parameters, and the performance of the system.[190]

The purpose of rendering the system explainable is different from technical transparency:[191]

- It enables the public purchaser to provide individuals or citizens with relevant information, on an individual level, to understand why the system reaches a specific decision or outcome (prediction, recommendation, ranking), allowing them to challenge such decision or outcome particularly in legal proceedings if necessary.
- It must be possible that public purchasers can explain individuals or citizens what changes must be made to the input to arrive to a different result.
- Unless the tender specifications expressly require otherwise, making the system explainable will in any event include a clear indication of the key factors that have led the system to a particular outcome and the changes that must be made in order to arrive at a different one.
- When preparing the specifications, the contracting authority may opt not to require the contractor to explain why the system arrives to a particular outcome, but the key factors that have led the system to such outcome. This provision is crucial because if the procured solution relies on black-box models, pinpointing the exact reasons for a specific outcome might be challenging. However, it remains feasible to identify the key factors that have contributed to the outcome.

Article 13(1) of the European Commission Standard Clauses also includes a specific provision imposing the obligation of the contractor to explain the functioning of the AI System on an individual level. This obligation encompasses the duty of the contractor, during the term of the Agreement to assist the public purchaser at its first request, to explain how the AI System arrived at a particular decision or outcome to the persons or group of persons on which the AI System is (intended to be) used. This assistance will include, at least, a clear indication of the key factors that led the AI System to arrive to a particular result and the changes to the input that must be made in order for it to arrive to a different outcome. As this specific obligation is complementary to the duty of transparency laid down in Article 6 of the Standard Clauses, it follows that the transparency requirement mandated by the AIA has not been conceived - at least in the Commission's approach - to ensure the explainability of high-risk AI systems.[192]

its parameters, and information on the performance of the Algorithmic System."

[188] See Amsterdam Standard Clauses, 9. "Explainable/Explainability" is defined as follows: "Being able to explain on an individual level why an Algorithmic System leads to a particular decision or outcome. […] this will in any event include a clear indication of the key factors that have led an Algorithmic System to a particular result and the changes to the input that must be made in order to arrive at a different result. Making an Algorithmic System Explainable includes the provision of all the technical and other information required in order to explain, in objection proceedings, appeal proceedings or other legal proceedings, how a Decision has come about and to offer the other party and any other interested parties the opportunity to assess the way in which a Decision has come about, so as to offer the other party realistic legal protection."

[189] See Article 5(1) of the Amsterdam Standard Clauses and the additional explanation to the provision.

[190] See Article 5(2) of the Amsterdam Standard Clauses and the additional explanation to the provision.

[191] See Article 5(4) of the Amsterdam Standard Clauses and the additional explanation to the provision.

[192] See European Commission Standard Clauses, 6, 9-10.

Given the flawed approach of the AIA to the requirements of transparency, interpretability and explainability of AI models, it is understandable that public procurement of AI solutions, in general, lacks the appropriate safeguards to adequately ensure that purchased COTS or bespoke solutions comply with these requirements. However, this could be highly problematic in the field of healthcare.

For example, the relevance the transparency requirement of the AI models has been highlighted by the AGENAS in relation to the provision of health services through telemedicine platforms and applications (Ref. [5]): "[…] it is crucial to adopt 'Transparent AI' systems and models, which allow physicians, healthcare managers and caregivers to have full visibility of the decision-making criteria adopted with the support of the system, while respecting the patient and the ethical complexity underlying clinical actions."[193] But the importance given to 'Transparent AI' seems insufficient. While the use of AI algorithms (such as machine learning and NLP for speech recognition) is expected to be implemented in this component to serve as decision-support tools for diagnosis and treatment of patients, the technical specifications do not include concrete provisions to ensure the transparency, interpretability and explainability of the predictive-modelling component of the platform.[194]

Only but a few tender specifications encompass requirements for contractors to ensure explainable AI.

For example, Lot 1 of the tender specifications published by the ECDC (ref. **[3]**) specifically required the contractor "to support ECDC with the implementation of artificial intelligence, including machine learning and deep learning, in the processes and tasks related to surveillance and other core public health functions, as well as the *related training required to properly handle and sustain these outputs* [emphasis added]." Notably, the deliverable DL9 was focused on "Explainable AI", the objective of which is to develop a R or Python code for explainable AI in order to improve the "interpretability of AI models". Additionally, Sub-deliverable 1 (DL9S1): "Development of R or Python code with local and/or global model-agnostic methods and specific methods for [Deep Learning] interpretation. Some examples of methods used can be found in: https://christophm.github.io/interpretable-ml-book".[195]

In the case of tenders in Annex II, none but three technical specifications include provisions addressed to ensure the explainability of the models.

Tender specifications	Requirements of explainability and interpretability
POPULATION HEALTH DATABASE (Ref. [13])	The platform must facilitate the interpretation and bias analysis of the artificial-intelligence models to be developed. The successful bidder must ensure explainability and bias reduction in all analytical models developed within the project to address the specified use cases.
INFOBANCO (Ref. [16])	The data-governance model (registration, access, and usage) will encompass "explainability and traceability requirements," aligning with

[193] AGENAS, *Proposta di partnership pubblico privato ai sensi degli artt. 180 e 183, c. 15, del Decreto legislativo 18 aprile 2016, no. 50 per l'AFFIDAMENTO DELLA CONCESSIONE per la progettazione, realizzazione e gestione dei Servizi Abilitanti della Piattaforma Nazionale di Telemedicina. PNRR - Missione 6 Componente 1 sub-investimento 1.2.3. "Telemedicina". Caratteristiche dei servizi e della gestione. Capitolato Gestionale*, 12 October 2022, 69, https://www.agenas.gov.it/.

[194] Idem, 70. In particular, the platform must incorporate a predictive modelling component (Sistema AI di Smart Suggestion) utilizing AI techniques such as NLP and Speech Recognition to serve as decision-support tools for diagnosis and treatment. Specifically, AI algorithms, leveraging patient-generated data including responses to questionnaires, chat messages, photos/videos of injuries/medications, and patient categorization, will generate active alerts correlated with information from stratified databases in regional and national health repositories. Recommendations from the AI models will guide healthcare personnel in specific actions for timely and appropriate support, whether health-related, psychological, or socio-sanitary, aimed at enhancing patient adherence to treatment pathways. The operational principle must be grounded in the systematic use of the Bayesian approach for calculating the ex-post probability of occurrence of the unknown event to be predicted ('likelihood' function), based on available evidence. This includes symptoms manifested by the patient during teleconsultation sessions (if present) or structured clinical observations recorded in the relevant Electronic Health Record (FSE 2.0), as well as experimental results from clinical efficacy trials for therapies targeting the patient's specific pathological conditions.

[195] ECDC, Tender Specifications, 11-12, 19.

	initiatives and future European regulations such as the Data Governance Act, European Health Data Space, Data Act, and AI Act.
PMED BIG DATA (Ref. [18])	The interpretability specified in the technical requirements pertains exclusively to the metrics of specificity (minimum false positives) and sensitivity (minimum false negatives). This requirement applies to use cases including home monitoring of chronic conditions and hospital discharges, therapeutic optimization, identification of opportunities for deprescription, and patient segmentation based on relevant pathologies.

Table 20. Explainability and interpretability in technical specifications

7.7. *Accuracy and performance metrics in tender specifications*

Trustworthiness of AI systems can be decomposed into several component properties, including accuracy, bias mitigation, transparency and explainability, privacy, resilience and security, reliability, robustness, and safety. There are different methods (metrics) to measure each property, its strengths and limitations or in what circumstances one metric would be preferable to another.[196]

As AI models provide a predictive output, accuracy is one of the paramount properties to be considered when such models are designed to be deployed in the healthcare context. The probability of a prediction can be interpreted as the "accuracy level" of the model. Put simply, if a given classifier (e.g. a convolutional neural network) predicts with 95% accuracy that a set of dots in a mammography image is a breast cancer, it could be said that the model has a "high accuracy classification". Otherwise, if the prediction is made with 55% accuracy, the algorithm could be said to have a "low accuracy classification".[197]

In this sense, accuracy is an AI system's property which refers to the system's ability to make correct judgements based on data or models. Accuracy of AI systems is an estimate of the closeness of a measured value to the exact value. High levels of accuracy are of paramount importance in situations where the AI system directly impacts human lives.[198]

The importance of this property is even stressed by some technical specifications in relation to AI-driven telemedicine solutions: "[…] the accuracy of the MD [Medical Device] is of great importance as it can seriously compromise the diagnostic process and endanger the patient's life" (Ref. [4]).

Accuracy then becomes critical to *correctly classify* mammography images for cancer detection (Ref. [11]), DAN variants for diagnosis of genetic diseases (Ref. [17]), healthcare demand for hospital and out-of hospital emergencies for patient triage (Ref. [8]); *make correct predictions* on morbidity in pandemic situation, epidemiological anticipation, forecasting, (Ref. [3]), weaning failure and length of stay in Intensive Unit Care (Ref. [19]); or *provide appropriate recommendations* for early warning of public-health threats (Ref. [3]) or to improve pharmacological treatment of complex chronic patients or surgery waiting lists (Ref. [13]).

In such cases, an evaluation process should be required to support, mitigate and correct unintended risks from inaccurate predictions, ensuring that error rates can be identified, measured and mitigated.[199] In this regard, performance metrics are used to measure the accuracy of the learning models by diagnosing their potential errors. Each metric has a specific technical interpretation, so it must always be linked to specific use cases.[200]

In this regard, when high-risk systems are engaged, the AIA stresses the importance of some of these components of trustworthy AI systems, including accuracy: "[…] if an AI

[196] AIME Planning Team, *Artificial Intelligence Measurement and Evaluation at the National Institute of Standards and Technology*, National Institute of Standards and Technology, June 2021, https://www.nist.gov. The OECD has published a catalogue of metrics to help AI stakeholders develop and deploy trustworthy AI systems. The list provides specific metrics to measure fairness, human well-being, privacy and data governance, robustness and digital security, safety, transparency and explainability. See OCDE, *Catalogue of Tools & Metrics for Trustworthy AI*, 2023, https://oecd.ai/. As of 11 November 2023, the OECD list covers 101 metrics.

[197] Cfr. ENISA, *Securing Machine Learning Algorithms*, 14 December 2021, 10, https://www.enisa.europa.eu.

[198] HLEG Ethical Guidelines, 17.

[199] *Ibidem*.

[200] S. Teki and A. Bajaj, *How to Improve ML Model Performance*, 29 September 2023, https://neptune.ai.

system is not trained with high quality data, does not meet adequate requirements in terms of its performance, its *accuracy* or robustness, or is not properly designed and tested before being put on the market or otherwise put into service, it may single out people in a discriminatory or otherwise incorrect or unjust manner (emphasis added)".[201]

In particular, it is critical to ensure that the performance of the models are consistent enough "throughout their lifecycle and meet an appropriate level of *accuracy*, robustness and cybersecurity in accordance with the generally acknowledged state of the art". For this reason, the AIA makes it mandatory to communicate the level of accuracy and accuracy metrics to the users or deployers of the AI system.[202]

In addition to robustness, cybersecurity, and consistent performance, accuracy (defined as "an appropriate level of accuracy") is one of the requirements for high-risk systems. Specifically, Article 15(2) of the AIA stipulates that "[t]he *levels of accuracy* and the *relevant accuracy metrics* of high-risk AI systems shall be declared in the accompanying instructions of use" (emphasis added). The original provisions of Article 13 of the AIA, which lists the relevant information to be included in the instructions of use, have been slightly modified in the Draft Agreement of the AIA. Accordingly, Article 13(b) requires that such instructions include, among other relevant information:[203]

- The level of accuracy, including its metrics.[204] robustness and cybersecurity against which the high-risk AI system has been tested and validated and which can be expected, and any known and foreseeable circumstances that may have an impact on that expected level of accuracy, robustness and cybersecurity;
- When appropriate, its performance regarding specific persons or groups of persons on which the system is intended to be used.

In the context of public procurement of AI systems for the NHCS, tender specifications should include specific requirements on accuracy thresholds. It is crucial to determine and verify the level of accuracy of AI models in relation to the task (classification or regression), its purpose, and the context of its use, bearing in mind that the expected performance of a model may vary. For example, in healthcare, classification models are often associated with diagnostics, being the class labels positive and negative. This would be the case of certain proteins associated with the risk of cancer. Then, when the classifier is run, it is possible to compare the list of true proteins (the ground truths) to the proteins recognized correctly or wrongly by the model (the predicted values). In this context, the trade-offs between "sensitivity" (also called "recall") and "specificity" metrics are critical. In particular, the ability to capture the true positive cases (sensitivity) may be particularly important if the AI solution is expected to be used in early breast-cancer screening tests. But at the same time, if sensitivity is overemphasised, the proportion of true negative cases correctly identified as such (specificity) would be unacceptably low. However, when reliable detection of positive cases is clearly important in a given context, the trade-off with sensitivity needs to be considered carefully.[205]

Moreover, trade-offs between precision and recall must be carefully addressed, as differences between them may affect the fairness of the model or may lead to adverse impacts.[206]

From the list of the tenders of interest, only some of them include specific provisions in the tender documents requiring the implementation of performance metrics. The joint procurement of Regional Governments of Valencia and Canarias, PMed Big Data (Ref. [18]), represents the best example of how performance metrics are required in relation to some use cases of Phase 1 of the

[201] Recital 38 of the AIA.
[202] Recital 49 of the AIA.
[203] In relation to the technical documentation required for high-risk AI systems, ANNEX IV of the AIA includes a detailed information about the metrics used to measure accuracy the monitoring (paragraph 2g); and the functioning and control of the AI system, "in particular with regard to its capabilities and limitations in performance, including the *degrees of accuracy for specific persons or groups of persons* on which the system is intended to be used and the *overall expected level of accuracy* in relation to its intended purpose; the foreseeable unintended outcomes and sources of risks to health and safety, fundamental rights and discrimination in view of the intended purpose of the AI system (emphasis added)."
[204] The reference to accuracy metrics was introduced in the AIA by an amendment of the Council mandate, and accepted in the Draft Agreement of January 2024.
[205] UK NHS Buyer's Guide, 34-36.
[206] Information Commissioner Office, *Guidance on AI and data protection*, version 2.0.17, 15 March 2023, 40, https://ico.org.uk.

project.[207]

USE CASE 7 (FHASE 1)- Description of the pathophysiology of low back pain using analytical prediction techniques from MR imaging
Minimum quality of model development in the first phase: the quality of the model will be determined on the basis of the following metrics: - Sensitivity: achieved 75%: 250 points. - Precision: achieved 75%: 250 points. - Accuracy: achieved 75%: 250 points. - F1 score: achieved 75%: 250 points. - The achievement of the milestone will be certified by the prediction of the delivered sample with an approximate accuracy of at least 75%. - Evaluation criteria for moving on to the second phase: the quality plus in terms of model development will be assessed using the following metrics: - Sensitivity: achieved 80%: 15 points; 85% achieved: 25 points. - Precision: achieved 80%: 15 points; 85% achieved: 25 points. - Accuracy: 80% achieved: 15 points; 85% achieved: 25 points. - F1 score: achieved 80%: 15 points; 85% achieved: 25 points.

Table 21. Accuracy thresholds in technical specifications

Completing this approach, for phase 2 of the project, technical specifications stipulated that, for each of the use cases, specificity (minimum false positives) and sensitivity (minimum false negatives) would be measured. By the end of June 10, 2023, the minimum values required by Spanish or European regulatory agencies for authorization as a diagnostic support device, were set at 95% and 90%, respectively. In at least half of the cases, it had to be reported that the prediction is of high probability and achieve 98.5% and 95% compared to human professionals.[208]

In the MEDIOGENOMICS project (Ref. [17]), tender specifications require that the automated retrieval and extraction of medical information must have a minimum quality of sensitivity and specificity, with errors in no more than 1% of text extractions and 2% of speech extractions.

In other tenders, technical specifications prescribe concrete metrics such as sensibility, specificity or the Area under the ROC Curve, but it does not stipulate any error thresholds (Refs. [8], [18]).

In many cases, users of AI systems emphasize model-error metrics while omitting the corresponding evaluation of the potential impacts of errors. For instance, a very low probability of error (e.g., 0.1% of false negatives), but with potential adverse impacts arising from this error (e.g., death of a patient), may not be assumable by the organization.[209]

8. *Concluding remarks: challenges for the NHCS in public procurement of AI solutions*

In general, procurement procedures must ensure the fulfilment of clinical and technical requirements, while also considering the pertinent regulatory and financial contexts.[210] In this respect, procurement procedures ought to serve as a mechanism to enhance efficiency, thereby fostering improved health outcomes. In addition, they should be used as a policy tool to achieve a range of objectives, including promoting innovation, supporting small and medium-sized enterprises, fostering sustainable growth and advancing social objectives such as building more inclusive public-health systems.[211]

A fresh and comprehensive approach on public procurement should be contemplated, shifting away from the rigid, bureaucratic administrative role - solely focused on obtaining work, supplies, or services - towards recognizing public procurement as a legal tool serving public purchasers to effectively fulfil the broader public interest and policies.[212]

More specifically, public procurement

[207] Gobierno de Canarias and Generalitat Valenciana, *Pliego de Prescripciones Técnicas*, 22.
[208] *Idem*, 25.

[209] A. Zlotnik, *Artificial Intelligence in Public Administrations: Definitions, Project Feasibility assessment and Application Areas* in *Boletic* (2019), no. 84, 2019, 27–28.
[210] S.C. Mathews, M.J. McShea, C.L. Hanley, A. Ravitz, A.B. Labrique and A.B. Cohen, *Digital health: a path to validation* in *NPJ Digital Medicine* vol. 2, no. 38, 2019, https://pubmed.ncbi.nlm.nih.gov/31304384.
[211] A. García-Altés *et al*., *Understanding public procurement within the health sector*, 172-185.
[212] European Commission, Europe 2020. A strategy for smart, sustainable and inclusive growth, Com(2010)2020, Brussels 3 March 2020; Council Conclusions. Public investment through public procurement: sustainable recovery and reviving a resilient EU economy, 2020/C 412I/01, Official Journal of the European Union, 30 November 2020.

should serve to design "a new architecture that allows the harmonious articulation of the so-called circles of excellence –service excellence (thinking first of people), process excellence (doing the right thing without undue bureaucracy) and technical excellence (having talent and knowledge)".[213]

Despite the beneficial outcomes, there are significant challenges that need to be addressed before any AI solution can be procured and deployed into public-health services.

The review of the sampled tenders reveals relevant challenges for NHCS in relation to the past, present, and future procurement of most AI solutions. These challenges can be classified on the basis of four criteria: the potential qualification of the procured solution as a high-risk AI system; the specific complexities of the procurement process in the healthcare sector; the legal and ethical risks due to the individual or societal impact of AI systems in healthcare; and the formal and substantive aspects of the procurement procedure and the design of tender specifications.

8.1. *The challenging interplay between the AIA and the MD Regulations and the problem of legacy systems*

At the macro level, there is no regulatory framework for AI with a sufficient level of development and maturity within the European Union, apart from fragmented national legislation.

The AIA is still under discussion. However, when planning the acquisition of AI-enabled solutions for the NHCS, the absence of a regulatory framework should not prevent contracting authorities from putting in place specific measures to adequately address inherent risks of AI acquisitions.

Moreover, once the AIA comes into force, it is likely to be quite challenging to bring legacy AI systems into full compliance with the EU Regulation's horizontal mandatory requirements for high-risk systems, irrespective of whether these systems are based on COTS or bespoke solutions.

For the time being, it remains unclear whether the AIA will be applicable or not to legacy AI systems already placed on the market or put into service before the effective date of application of the Regulation.[214]

However, if the Act is ultimately applicable to such legacy systems,[215] it is likely to be quite challenging to bring them into full compliance with the AIA, irrespective of whether those systems are based on COTS or bespoke solutions.

8.2. *Complexities of procurement process can be exacerbated by AI*

At the micro level, contracting authorities will face specific challenges.

In the first place, the role of public administrations as guarantors may determine the deployment of different AI applications in the NHCS than in the private sector.[216] In this sense, healthcare is a highly sensitive area, where AI-enabled solutions must be designed for public use in order to meet the needs of all citizens. Whereas such constraints are not necessarily present in the private sector, public-sector purchases should be in the public interest, which means higher standards of compliance.[217]

In the second place, the purchase of AI solutions by public-health services also poses a major challenge in terms of planning and design of these procurement procedures, as many highly complex transactions are involved. To a greater or lesser extent, the disruptive nature of AI is beginning to shape the existing procurement processes, given that "uncertainty" is a dominant feature of AI solutions in terms of functionality, behaviour and organizational consequences.[218]

At the same time, such uncertainty may

[213] J.M. Gimeno Feliú, *El necesario big bang en la contratación pública: hacia una visión disruptiva regulatoria y en la gestión pública y privada, que ponga el acento en la calidad*, in *Revista General de Derecho Administrativo*, no. 59, 2022.

[214] Cfr. Article 83 of the AIA. With the exception of the effective date of application of the AIA (12 or 36 months before its entry into force), the Council's version contains the same provisions as the Commission's with regard to AI systems already placed on the market or put into service.

[215] In line with the demands of the EU Parliament, European Economic and Social Committee, European Data Protection Supervisor or European Data Protection Board.

[216] I. Georgieva, T. Timan and M. Hoekstra, *Regulatory divergences in the draft AI Act. Differences in public and private sector obligations*, European Parliamentary Research Service, Brussels, May 2022; M. Manzoni, R. Medaglia, L. Tangi, C. Van Noordt, L. Vaccari and D. Gattwinkel, *AI Watch. Road to the Adoption of Artificial Intelligence by the Public Sector*, JRC-European Commission, Luxembourg, 2022.

[217] M. Sloane *et al*., AI and Procurement, 7-8.

[218] L. Silsand *et al*., *Procurement of artificial intelligence for radiology*, 1388, 1389.

trigger potential challenges during the procurement process of AI solutions for NHCS in relation to the selection of the adequate procurement procedure and/or the design of the tender specifications to put in place appropriate safeguards in order to ensure trustworthiness and iterative evaluation of the purchased AI solution.

In the third place, public-health purchasers often lack extensive knowledge of existing solutions on the market or may not be aware of the specific public needs to be addressed, or the optimal technological solution for the problem at hand. There may also be an imbalance between purchasers, public-health services, and suppliers, particularly due to existing barriers that hinder competition and limit the number of economic operators bidding for tenders. Similarly, difficulties may arise regarding the ownership of intellectual property resulting from AI products or the incorporation of interoperable solutions that prevent vendor lock-in.[219]

In the fourth place, the quality of the AI solutions purchased is highly dependent on technical requirements, such as having standardised and secure repositories of multidimensional data, ensuring the accuracy of the AI models over time, industrialising the deployment and control of the models, or ensuring the security and confidentiality of the data throughout the lifecycle of solutions.[220] Furthermore, to understand how the diagnosis, prognosis or treatment pathways are reached, thereby increasing the buy-in from medical staff, an adequate degree of transparency and interpretability is needed over the results produced by AI systems.[221]

Finally, contracting authorities should be provided with appropriate human and material resources "to build up literacies and capacities" around the collective and individual impacts of procuring AI solutions. This literacy and capacity building should include the exchange of expert knowledge across public buyers.[222]

8.3. *Legal and ethical risks of AI solutions*

At the macro-level, there are also many legal and ethical challenges associated with the use of AI in health sector.

Because of the sensitive nature of healthcare, it is not a coincidence that the future AIA will set forth specific rules for AI systems that can create a high risk to "health and safety or fundamental rights of natural persons", regardless that they operate as stand-alone systems or components of products (e.g. medical devices).[223]

*Prima faci*e, AI solutions are prone to collide with fundamental rights enshrined by the Charter of Fundamental Rights of the European Union (EU Charter) and the constitutional texts of the Member States. This could be the case of the right to privacy and personal-data protection,[224] insofar as these AI applications would process particularly sensitive data of citizens such as health data.[225] By the same token, the right to equality and non-discrimination[226] could be compromised, given the risk of classifying or stratifying patients into groups or subgroups according to the processing of data by AI solutions resulting in discriminatory or stigmatising decisions.

From an ethical perspective, the dilemma will always be "who" and "what" the AI is used for,[227] along with considerations of transparency, lack of bias, inclusiveness, etc.[228]

---

[219] See European Commission, *Public procurement in healthcare system: Opinion of the Expert Panel on effective ways of investing in Health (EXPH)*, Luxemburg, Publications Office of the European Union, 2021, 1, 8, Doi:10.2875/832331; García-Altés *et al*., *Understanding public procurement within the health* sector, 172-185.

[220] J.C. Sanchez Rosado and M. Diez Parra, *Impacto de la inteligencia artificial en la transformación de la sanidad: beneficios y retos*, in *Economía industrial*, no. 423, 2022, 129-144.

[221] Harwich and Laycock, *Thinking on its own*, 24, 42-43.

[222] M. Sloane *et al.*, *AI and Procurement*, 28.

[223] See Recitals (27), (28), (43), and Article 6 in relation to Annex II. 8 and Annex III. 5 of the AIA.

[224] Respectively, Articles 7 and 8 of the EU Charter.

[225] L. Cristea Uivaru, *The protection of sensitive data: Digital Health Record and Big Data in Health*, Barcelona, J.B. Bosch Editor, 2018.

[226] Articles 20 *et seq*. of the EU Charter.

[227] A cancer-predictive model used by the public health system to make early diagnoses is not the same as an AI model used by an insurer to grant or deny a health insurance or, even to determine the health insurance premium. See S. Hoffman and A. Podgurski, *Artificial intelligence and discrimination in health care*, in *Yale Journal of Health Policy, Law and Ethics*, vol. 19, no. 3, 2020, 1, 31; C.W.L. Ho, J. Ali and K. Caals, *Ensuring trustworthy use of artificial intelligence,* in *Bulletin of the World Health Organisation*, vol. 98, no. 4, 2020, 263, 264.

[228] World Health Organization, *Ethics and governance of artificial intelligence in health: WHO guidance: summary*, 2021, https://apps.who.int/iris/handle/10665/350263.

8.4. *Addressing formal and substantive challenges of AI procurement for the NCHS*

Deciding whether or not to procure AI solutions for the NHCS and drafting tender specifications could be challenging, as it is necessary to avoid potential tensions that may arise between the formal aspects (the procurement process) and the substantive aspects (including specific safeguards in the tender specifications to mitigate the specific risks of procuring an AI solution to meet a public need). In between, an ex-ante AI impact assessment will help to identify the specific individuals, targeted patients or societal risks of the AI solution.

On the one hand, the formal aspects of the procurement process require the public purchaser to take strategic decisions on whether AI is the best solution to meet the public need identified by the public purchaser, the appropriateness and feasibility of implementing an innovation procurement approach (PPI or PCP), an adequate analysis of the state of the art, and market engagement to launch open-market consultations, the type of procedure to be used (open or specific innovation procedures), the expertise and multidisciplinarity of the public officials in charge of evaluating the bidders' offers, whether to acquire a COTS or a bespoke solution, the type of tender specifications (descriptive or functional), the appropriate management of intellectual-property rights.

On the other hand, tender specifications should consider specific safeguards to avoid the inherent risks of implementing AI in healthcare in relation to the identified use cases. An ex-ante AI impact assessment will enable public purchasers of the NHCS to proactively detect potential risks and design appropriate technical and organisational measures and safeguards to be implemented in tender specifications.

Irrespective of whether the AI system is classified as "high risk" or not, the public purchaser should ensure that the technical and administrative specifications include appropriate provisions, including safeguards in line with the future AIA, to ensure: the quality and validation of data sets for the intended purpose, the integration and interoperability of the AI solution with the existing infrastructure and organisational practices of the health service, technical and procedural transparency and explainability approach to ensure an adequate level of interpretability of the AI solution in relation to the end user of the system and the individuals or collectives concerned, human oversight, robustness and security, adequate metrics to minimise errors and optimise the performance of the procured solution, full compliance with the intended purpose throughout the life cycle of the AI system, a documented risk-management system in relation to the specific risks of the AI solution, and technical documentation of the procured solution to be provided by the contractor in a timely manner.[229]

[229] Final note from the authors: At the time of publication of this work, the European Parliament had adopted the final version of the AIA (See legislative resolution of 13 March 2024, P9_TA(2024)0138). Consequently, references in this work to the AIA in the Commission's proposed version (COM/2021/206 final) or the trilogue text (Draft Agreement of 21 January 2024) may have changed.

9. *Annexes: tenders of interest*

9.1. *Annex I: eTendering (EU) and Ministero della Salut (Italy)*

Contracting authority	Subject-matter	AI strategy	Procurement innovation strategy/ Procedure type	Awarded
Notice Reference: Ref. [1]. SMART 2019/0056				
European Commission DG CONNECT	Study aiming to analyse the progress on the adoption of AI technologies for the benefit of patients and EU healthcare sector, and to provide an overview of the current situation across EU Member States, with a view to support and inform EU policy initiatives to harness AI and Big Data for digital transformation and improvement of EU healthcare (Lot 2).	Review of relevant available data, surveys, methodologies, indicators and metrics in EU healthcare sector.	Open Procedure	23/09/2019 (Closed) No info on contractor in eTendering
Notice Reference: Ref. [2]. OC/EFSA/AMU/2020/02				
European Food Safety Authority (EFSA) and other EU bodies	Providing assistance to EFSA for statistical and epidemiological analyses, related data management and other relevant tasks using AI methodology, as well as for training and *ad hoc* consultation upon request.	AI and MLT models e.g. NLP, text classification, NER models etc.).	Open Procedure	25/11/2020 (Closed) No info on contractor in eTendering
Notice Reference: Ref. [3]. OJ/2023/PHF/26497				
European Centre for Disease Prevention and Control (ECDC)	Implementation of AI in the processes and tasks related to surveillance and other core public-health functions, with further improvement of early warning of public-health threats using social media, as well as the related training required to properly handle and sustain these outputs.	ML/DL model for regression or classification problem. Unsupervised models on clustering or dimensionality reduction. NLP models. AI interpretability methods.	Open Procedure Framework Agreement	01/09/2023 (closed) No info on contractor in eTendering
Notice Reference: Ref. [4]. CIG 94572555B6				
Italian National Agency for Regional Healthcare Service (AGENAS)	Design, implementation, deployment and management of an AI platform to support primary health care.	ML, DL, Federated learning.	Competitive dialogue Piano Nazionale di Ripresa i Resilienza	No info Deadline for tenders: 16/12/2022
Notice Reference: Ref. [5]. CIG: 9423681B90				
Italian National Agency for	Design, implementation and management of the enabling services of	ML (Bayesian approach), NLP, NPL-	Open Procedure Piano Nazionale	01/03/2023

Regional Healthcare Service (AGENAS)	the National Telemedicine Platform for fast data access to be processed and updated, both through traditional techniques and innovative approaches (AI di Smart Suggestion), which include a teleconsultation module integrating NLP, Augmented Reality and predictive modelling.	speech recognition (speech-to-text-to-analysis), Augmented Reality.	di Ripresa i Resilienza	

9.2. *Annex II: PLACE and buyer profiles (Spain)*

Contracting authority	Subject-matter	AI strategy	Procurement innovation strategy/ Procedure type	Awarded
Notice Reference: Ref [6]. 123/15-SV				
State public undertaking, Red.es	Information system under Big Data architecture for sentiment analysis of the Regional Health Service of Castilla-La Mancha (SESCAM).	Classification algorithms.	Open Procedure	22/09/2015
Notice Reference: Ref. [7]. 2016/051				
National Institute for Health Management (INGESA)	R&D to build a clinical information repository and 4 expert systems (hypercholesterolaemia, diabetes mellitus, emergency and telemonitoring of chronic patients) for predictive analysis and decision-support based on the repository.	No information available on PLACE (only prior contract notice).	PCP Open Procedure	No info available on PLACE.
Notice Reference: Ref. [8]. CNMY18/AVSRE/4				
Presidency of the Regional Govt' of Valencia	Expert system to assist 112 operators in the classification of healthcare demand for emergencies, out-of-hospital emergencies and medical calls to emergency number 112.	Naïve Bayes, FAN, TAN, neural networks and other algorithms with best performance.	Open procedure	12/06/2018
Notice Reference: Ref. [9]. 2023-PR-036 (2019-3-009)				
University Hospital Infanta Leonor	Development, support and maintenance of an advanced expert healthcare support system, implemented with AI, for the exploitation of the information (Big Data) contained in the hospital's electronic medical records.	NLP, ML, neural networks.	Negotiated procedure without publication	22/06/2019
Notice Reference: Ref. [10]. LN-SER1-18-041				
Galician Health Service (SERGAS)	Personal-assistant system (AVATAR) which generates intelligent alert generator to increase patient autonomy.	(Undetermined) AI techniques for pattern behaviour detection and advanced system for facial, body posture and voice recognition .	Negotiated procedure	24/06/2019
Notice Reference: Ref. [11]. DC-SER1-19-003				
Galician	Support system for cancer detection	(Undetermined)	PPI	27/09/2019

Health Service (SERGAS)	(CADIA) based on the analysis of mammography and pathological anatomy imaging with AI techniques.	Optimal statistical analysis method.	Competitive Dialogue	
Notice Reference: Ref. [12] 2020/LIC/0026				
EGARSAT, Auxiliary entity of the Social Security System	Design, development, implementation and maintenance of AI-based support-information decision systems for predicting the duration of sickness absence due to illness or accident; predicting the number and type of sickness absence 12 months ahead and segmenting it by diagnosis, cause and month; ongoing maintenance of predictive models for 3 to 4 years.	ML (Regression, Clustering, Classification, Recommendation), ANN, Random Forest, SVM.	Open Procedure	24/09/2020
Notice Reference: Ref. [13]. 067/20-SP				
State public undertaking, Red.es	Corporate solution (software and hardware platform) for advanced analytics based on Big Data, ML and DL technologies for the Public Health System of Andalusia (SAS), enabling massive exploitation of the 'Population Health Database'.	ML, DL.	Open Procedure	02/08/2021
Notice Reference: Ref. [14]. CSE/9900/1101001998/21/PA				
Health Service of Murcia (SMS)	Design, implementation, setup and development of a health-data lake platform in the Health Service of Murcia (AZUD Project).	ML.	Open Procedure	18/11/2021
Notice Reference: Ref. [15]. 202150PA0009				
Ministry of Health	Development of applications for digital transformation in the National Health System of the Ministry of Health.	Analytical tools, AI, NLP, other (Big Data, Blockchain, Robotics).	Open Procedure National Plan of Recovery, Transformation and Resilience	11/03/2022
Notice Reference: Ref. [16] 51/2021 (A/SER-032254/2021)				
Health Dpt.' of the Regional Govt.' of Madrid	Development and implementation of a three-layer Data Lake architecture (INFOBANCO) for health system learning, conceived as a standardised repository of health data generated by different sources (clinical, administrative and research systems), for care improvement and innovation, personalised medicine, biomedical research and other secondary uses.	Tools for building analytical and predictive models based on statistics (statistical learning) and computer science (machine learning, deep learning, AI), federated learning.	PPI Open Procedure	22/03/2022
Notice Reference: Ref. [17]. 52/2021 (A/SER-032253/2021)				
Health Dept.' of the Regional Govt.' of Madrid	Expert platform (MEDIOGENOMICS) that automatically combines the entire process of an individual's genomic study, clinical information obtained	Automatic retrieval and encoding of relevant clinical data from electronic/ paper reports and consulta-	PPI Accelerated open procedure	29/03/2022

	during consultation and massive sequencing of 380 genomes using NGS with continuous updating in real time and integration with EHR, aimed at optimising genetic diagnosis for the patient/citizen and improving diagnostic tools for genetic diseases.	tions (speech-to-text) using NLP and ML techniques. Analysis of genomic information contained in EHR with ML techniques.		
Notice Reference: Ref. [18] 18/CPP/1				
Health Depts.' of the Regional Govts.' of Gran Canarias and Valencia	Development of an interoperable solution, «MEDICINA PERSONALIZADA BIG DATA», («PMed Big Data») integrating (i) a patient-health system interface for data collection to register lifestyle and promotion of health, assisted by AI; (ii) predictive clinical tools for support decision; (iii) a platform that operationalises available data into useful functionalities for patient care. The interface and support-decision tools will respond to the listed use cases and meet specific objectives (personalized treatments and early diagnose, reduction of adverse effects, effectiveness of treatments for complex chronic patients, improvement of healthcare resources).	NLP, ML/DL.	PCP Open procedure	06/04/2022
Notice Reference: Ref. [19]. CSE/AH02/1101308996/23/PO				
Catalan Institute of Health (ICS)	Development of AI models on the Data Lake type historic repository available at the proprietary Cloudera Platform to improve and support clinical-decision making in the integral care of critical patients and their families (CRITIC-CONTAS) according to the expected use cases (prediction of weaning failure, length of stay in ICU) and optionally (prediction of shock, cardiorespiratory arrest, coma, respiratory failure, discharge from the ICU to the ward).	ML, DL.	Open Procedure	06/06/2023
Notice Reference: Ref. [20] ROSIA PCP 101017606				
Health Sciences Institute of Aragón and others	New solutions to be developed and tested to address and unlock the tele-rehabilitation market by purchasing the development of a technologically-innovative ecosystem, enabling service providers to provide telerehabilitation, and self-management of rehabilitation & self-care at home, at scale.	AI analytics/ML, Augmented Reality.	PCP Open procedure	29/09/2022

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 141-145
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 09

*Tele-doctors? Navigating the Future of Healthcare: Advantages and Risks of AI-Enhanced Telemedicine**

Carlo Casonato
(Full Professor of Comparative Constitutional Law and Jean Monnet Chair on EU Law of AI (T4F) at University of Trento)

ABSTRACT The article explores the benefits and drawbacks of AI-supported telemedicine tools. Utilizing a case study as a focal point, it evaluates their implications on patient rights, the physician's role, and the broader landscape of medical practice

1. *Introduction*

According to the latest literature, the term "telemedicine" was first used in 1971 by a Boston doctor who had established a "microwave link" to remotely connect an urgent care clinic to the emergency department of the Massachusetts General Hospital.[1] Preceded by a decade-long experience with less sophisticated devices such as the telephone, this technology quickly spread. Following a series of technical improvements, it gained support from the US Department of Health.[2]

As early as the 1950s, projects were underway to condense disease characteristics into computer-processable information (bits) to assist doctors in decoding and interpreting a vast amount of otherwise overwhelming data. The motto of the time was encapsulated in phrases like "Electronic medical journals, electronic diagnostic machines, electronic medical records," with the risk that doctors might become mere "Push-Button Physicians".[3] Even during those years, the advantages of this novel approach were highlighted, emphasizing its liberation from distances, speed, and comprehensive analysis. However, certain limitations were identified from the outset, leading the director of the National Library of Medicine to assert, in 1964, that the new devices were "a new instrument of the research library, not a replacement".[4]

Following a period of progress slowdown in the field of "electronic medicine," which roughly corresponded to the so-called "winter of artificial intelligence," funding in the sector was limited. However, with the advent of the new millennium, the extraordinary computational power of modern computers and emerging technologies (machine learning, neural networks, etc.) enabled the rapid processing of massive amounts of data, including health-related data that every individual leaves behind throughout their life. With a surge in sector investments, Artificial Intelligence (AI) became the technology with the fastest rate of adoption in medicine, unlocking significant advantages while also harboring notable risks.

In this short article, I will address some of the many issues related to the use of AI in medicine.

2. *GP at Hand*

The impact of the Covid experience and the subsequent erosion and depersonalization of many relationships have brought to the forefront the strengths and vulnerabilities

* Article submitted to double-blind peer review.
The article is a revised and updated version of the piece published in Italian Telemedicina. Vantaggi e rischi della telemedicina assistita da intelligenza artificiale, in E. Rigo (a cura di), Per una ragione artificiale. In dialogo con Lorenzo d'Avack su Costituzione, ordine giuridico e biodiritto, RomaTre Press, 2023, 219-227. Some of the presented points are part of the activities of the NextGenerationEU project (FAIR - Future AI Research - PE000013) co-funded by the European Union, and the national funded project Medicine+ (AI, Law and Ethics for an Augmented and Human-Centered Medicine - PRIN 2022). The views and opinions expressed are solely mine and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

[1] J.A. Greene, *The Doctor Who Wasn't There*, Chicago, The University of Chicago Press, 2022, 3.

[2] R.L. Bashshur and G.W. Shannon, *History of Telemedicine. Evolution, Context, and Transformation*, Mary Ann Liebert Inc., 2010.

[3] J.A. Greene, The Doctor Who Wasn't There, 181.

[4] *Ibidem*, 187.

inherent in remote healthcare delivery.[5] A compelling case that exemplifies the advantages and pitfalls of integrating AI into the realm of patient care relationships is *GP at Hand* by Babylon — a sophisticated "intelligent medical assistance" system already operational in select regions across the UK, the US, and Africa. This system, taken over by US company eMed after the financial difficulties encountered by Babylon Health,[6] empowers participating General Practitioners (GPs) to swiftly and accurately generate diagnoses, prognoses, and treatment pathways for patients who opt for this mode of healthcare. To comprehensively assess the potentials and ambiguities of this service, I will propose an analytical framework that commences with a short exposition of the mentioned application (GP at Hand) and subsequently delves into its potential ramifications for patients, medical professionals, and the broader field of healthcare.

GP at Hand stands is part of a strategic initiative embraced by the British government and others, aimed at broadening access to high-quality primary care through the integration of digital technologies. One key facet of this initiative is the access to an online video consultation service, facilitated by an app developed by Babylon Health — a private enterprise affiliated with the National Health Service (NHS) now substituted by eMed.[7] Individuals electing to register for this service embark on an initial phase of automated consultation, after which they can decide whether to activate a video consultation with a doctor. The app extends its accessibility around the clock (24/7), ensuring that a remote consultation with a physician can be secured within an average timeframe of four hours. In scenarios where this mode of consultation fails to meet expectations, patients retain the option to schedule a conventional in-person visit with a physician affiliated with the NHS, adhering to standard protocols and waiting periods.[8]

One of the key features of the service is that the remote examining physicians are assisted by an AI mechanism, which allows them to access the patient's medical history and their digital twin. Based on this data and the course of the dialogue, the system offers real-time suggestions for questions to be posed to the patient. This helps to clarify potential causes of the reported discomfort, make a diagnosis, provide a prognosis, and propose a treatment plan during the "visit". Furthermore, a facial recognition system is employed to detect the patient's emotional states (such as confusion, boredom, or concern), thereby guiding the physician in employing the most suitable communication strategies for conducting a precise and effective interview. The dialogue is automatically transcribed and recorded, remaining within the company archive and accessible to the patient.

This model presents both potentials and uncertainties, which, as previously mentioned, can be examined from the standpoint of their impact on the patient, the physician, and the field of healthcare as a whole.

3. *The patient*

First, the advantages for the patient are evident, particularly in terms of the speed of consultation. This is due to the operational mode of the provided service (24/7) and the opportunity to secure a video consultation within a few hours. Secondly, the AI system's ability to correlate the patient's medical history with insights gathered during the conversation, coupled with statistically probable outcomes derived from extensive databases, enables the formulation and suggestion of diagnoses, prognoses, and treatment proposals with a high degree of accuracy. Thirdly, concerning the patient-care relationship, facial recognition brings the advantage of assisting the physician in understanding the patient's reactions, thereby facilitating the adjustment of communication methods and overall comprehensibility.

However, this system also carries a set of inherent risks. For instance, it's widely acknowledged that AI systems incorporate and generate significant errors and biases.[9]

[5] See National Academy of Medicine, *Toward Equitable Innovation in Health and Medicine: A Framework*, Washington, DC, The National Academies Press, 2023.

[6] See E. Mahase, Babylon looks to sell GP at Hand and other UK business amid financial issues, in BMJ, 2023, 382; S. Trendal, New owner of remote NHS GP service pledges no disruption or staff cuts after Babylon bankruptcy, in Health and Social Care, News, Oct 4, 2023.

[7] Cfr. www.england.nhs.uk/london/our-work/gp-at-hand-fact-sheet/#:~:text=Babylon%20GP%20at%20Hand%20is,point%20of%20use%20for%20patients.

[8] T. Burki, GP at hand: a digital revolution for health care provision?, in The Lancet, 2019, 394, 457.

[9] M. Burges and N. Kobie, The messy, cautionary tale

These problems stem from both the human factor in constructing the system and selecting training datasets, as well as from algorithmic results and their respective interpretations. A second problem pertains to the non-equivalence between an audio-video connection (guided by an AI system) and an in-person medical visit.[10] In this sense, the app could contribute to a dehumanization of the doctor-patient relationship, where both parties content themselves with interacting solely with a virtual component. A third layer of concern is tied to the requirement that patients using *GP at Hand* possess strong digital skills. This element leads to a selective effect on individuals engaging with the system, which transcends the digital divide and impacts age and consequently the general health condition of patients, as well as their socioeconomic background and corresponding income.[11] This condition thus risks generating a potentially discriminatory effect based on both users' age and social status.[12]

4. *The physician*

The advantages and challenges of the examined application can also be assessed in relation to the physician utilizing it. On a positive note, this system allows the healthcare professional to choose their available time slots. The 24/7 mode, in fact, offers considerable flexibility in defining one's work hours, eliminating the need to adhere to standard schedules. However, it's worth noting that this flexibility is underpinned by the demand-to-supply logic. Some doctors might, in reality, find themselves compelled to work inconvenient hours. Among the benefits for the professional, it's worth also mentioning that *GP at Hand* provides the opportunity to perform their duties wherever a sufficiently strong network exists, minimizing unnecessary travel and enabling them to set up their "office" in any location.

Conversely, considering the aforementioned characteristics of the population segment that typically turns to the app in question (young individuals with higher income), *GP at Hand* could also have a discriminatory impact in reference to the medical field. Professionals participating in this initiative might end up treating wealthier and younger individuals (who statistically have better health conditions), leaving "traditional" colleagues to handle patients with more complex and demanding medical needs. Such a trend could be counterproductive for the doctors themselves who participate in the remote service: accustomed to dealing with the easier population segment, they might risk gradually losing their ability to address more serious and complex health issues, undergoing an overall process of de-skilling.

In a similar light, there's a risk that physicians, supported by the AI system in their activities, could fall into a routine where clinical decisions are effectively delegated to the machine. In an era of widespread, albeit mistaken, perception of technology as neutral, objective, and infallible, the *GP at Hand* doctor might find it more comfortable and prudent to not contest the algorithmic outcome, avoiding potentially risky personal responsibility.[13] The threat, in essence, lies in the substantial capture of clinical decision-making by AI,[14] potentially generating a new model of defensive medicine.

On the other hand, in a broader context, some observers believe that the use of AI in medicine encourages physicians to reclaim a central role in the doctor-patient relationship.

of how Babylon disrupted the NHS, in Wired, 18 March 2019 (www.wired.co.uk/article/babylon-health-nhs). In general, see: D.A. Vyas et al., Hidden in Plain Sight — Reconsidering the Use of Race Correction in Clinical Algorithms, in New England Journal of Medicine, 2020, 874-882; A. Bracic et al., Exclusion cycles: Reinforcing disparities in medicine, in Science, 2022, 6611, 1158-1160.

[10] K.E. Karches, The Moral Difference between Faces & Face Time, in The Hastings Center Report, 4/2023, 16-25.

[11] 94% of individuals who turned to GP at Hand are under the age of 45, and two-thirds of them come from affluent residential areas: T. Burki, *GP at hand: a digital revolution for health care provision?*, cit. 458; M. Burges and N. Kobie, *The messy, cautionary tale of how Babylon disrupted the NHS*, cit.

[12] L. d'Avack, *La rivoluzione tecnologica e la nuova era digitale: problemi etici*, in U. Ruffolo (dir.), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, 21 mentions the need for the opportunities of new technologies to be inclusive of as many citizens as possible regardless of their social status, income class, geographical location and other similar factors.

[13] "The collective medical mind is becoming the combination of published literature and the data captured in health care systems, as opposed to individual clinical experience", according to D.S. Char, N.H. Shah and D. Magnus, *Implementing Machine Learning in Health Care – Addressing Ethical Challenges*, in *The New England Journal of Medicine*, 2018, 378(11), 981.

[14] A. Simoncini, L'algoritmo incostituzionale: intelligenza artificiale e il futuro delle libertà, in BioLaw Journal – Rivista di BioDiritto, no. 1, 2019, 69.

This allows for delegating less crucial tasks to machines while concentrating on activities where a human element is essential.[15] In these terms, the app could free healthcare professionals from the routine aspects of visits, enabling them to dedicate more time to complex cases and to revive the interpersonal dimension of their profession. Conversely, other commentators have analyzed historically established trends regarding medical workloads, identifying that the reduction in tasks does not necessarily correspond to an increase in time allocated to the remaining tasks but often results in a higher number of services to be delivered.[16]

5. *Medical practice*

The considerations discussed so far introduce the changes that the use of AI, as exemplified by *GP at Hand*, could bring about in medical practice. Among the numerous advantages, the following can be highlighted: the potential to re-organize healthcare services in a more flexible and effective manner, promptly and competently addressing the growing demand for health; assisting general practitioners (but not limited to them) in arriving at swift and accurate diagnoses and treatment paths; providing an opportunity to restore a central role for physicians in the care relationship; and the ability to structure a sustainable, patient-oriented approach to medicine. On a global scale, furthermore, the use of AI can be highly effective, especially in reference to middle- to low-income countries, where the ailing population would otherwise have no access to medical care.[17]

Alongside these opportunities, the use of AI in medicine does, however, raise a series of questions and doubts. First, the risk of potential atrophy in face-to-face visits (de-skilling) has surfaced, with the danger of an overall dehumanization of healthcare that could transform it into a sort of sophisticated "call center". Additionally, the provision of the app by private companies such as Babylon or eMed might drive the marginalization of the public dimension in a sector where economic and financial interests prevailing over those related to collective health cannot be ruled out. There's a potential risk, for example, that algorithms programmed according to criteria oriented towards commercial speculation rather than the enhancement of public health could foster increased consumption of (specific) drugs, thereby elevating healthcare expenditure. Instead of promoting, for instance, strategies related to change in lifestyles. Concerning the overall economic sustainability of *GP at Hand*, it has also been observed that the ease of accessing video consultations could lead to an increase in demand (supply-induced demand).[18]

Furthermore, when referring to more sophisticated AI techniques such as machine learning, it becomes practically impossible to trace the internal steps and underlying logic adopted by the machine to reach the output. While the final outcome of the process is known, the sequence that generated it remains obscure due to the inherent opacity of the internal dynamics of the system.[19] This phenomenon, the black box problem, holds particular significance in the medical field as well. It hinders the examination and potential adjustment of individual internal phases of the procedure and compromises the ability to scrutinize the congruence of the reasoning behind the decision. In the absence of transparency, there arises a strong doubt whether clinical decisions can truly enjoy full legitimacy and comprehensive recognition from patients.

Another potentially critical impact of employing *GP at Hand* on medicine pertains to its validation. As medical devices, these apps might follow well-defined paths of clinical trial. However, specific characteristics of these devices warrant special attention. In particular, mechanisms based on machine learning have the ability to adapt their functioning based on experience. Therefore, even if a device had initially been granted authorization for use, one must question how long such approval remains valid when the

[15] E. Topol, Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again, New York, Basik Books, 2019.

[16] R. Sparrow and J. Hatherley, High Hopes for "Deep Medicine"? AI, Economics, and the Future of Care, in The Hastings Center Reports, 2020, 50, no. 1, 14-17.

[17] Babylon has announced its intention to extend the operation of the app to eleven Asian countries in addition to the United States. In Rwanda, also thanks to a grant from the Bill & Melinda Gates Foundation, the system is used by about two million people, at a one-off price of 20 cents. See T. Burki, *GP at hand: a digital revolution for health care provision?*, *supra*, 460.

[18] *Ibidem,* 459-60.

[19] See F. Pasquale, *The Black Box Society*, Cambridge MA, Harvard University Press, 2016.

device itself has autonomously modified its operations.[20]

In more general terms, moreover, the question has been raised whether AI devices employed in the medical field should not be evaluated in light of a far broader spectrum of interests beyond their mere technical efficacy and security. As exemplified by *GP at Hand* itself, the utilization of such devices yields an impact that extends well beyond the therapeutic benefit of an individual service for a single patient. It engulfs a plethora of collective dimensions and variables spanning social, legal, professional, and economic realms. What warrants concern, therefore, is not only the potential harm to individual users (physicians or patients), but also the overarching models of medicine (and society) that the dissemination of these tools inherently carries.

6. *Concluding remarks*

What has been argued so far certainly does not lead to rejecting new AI technologies in the medical field. Instead, it urges us to reflect on the necessary precautions to avert risks and harness benefits.

First and foremost, it is imperative to prevent algorithm-assisted medicine from exacerbating existing social and economic vulnerabilities rather than addressing them. Effective tools must also be devised to ensure that professionals working with AI do not lose their familiarity with the principles underpinning human relationships, countering the trend of de-skilling that has emerged in the execution of other tasks. The economic and financial aspects involved must also be carefully evaluated to maintain a balanced system between the public and private domains.

Moreover, there is a crucial need to invest in educational and awareness initiatives aimed at both the general population and healthcare professionals. On the societal front, this approach will raise awareness about the potential benefits as well as the critical aspects of AI, preventing, for example, the generation of illusions about the infallibility of algorithmic medicine or the realization of risks associated with automation bias. On the professional side, it is important to strengthen interdisciplinary training paths, ensuring that physicians are not tempted to delegate their role to machines. To give a concrete and safeguarding meaning to the principle of "Human in the Loop" it's not enough to merely include humans in the process of forming medical decisions. Instead, these individuals must possess basic computer skills to interpret algorithmic decisions and have the authority and willingness to play a role of effective oversight in the diagnostic and treatment journey.[21] Otherwise, there's a risk that AI-linked medicine, even within the realm of current defensive medicine trends, might reinforce a hazardous process of medical de-humanization and de-responsibilization.

Returning to introductory reflections dedicated to the human element that must characterize law, ethics, and medicine, it can be concluded by emphasizing the necessity of "defending human specificity in relation to machines".[22] This recognition comes with the awareness that "science and technology alone will never be able to deliver a more just and equitable society".[23]

[20] In this respect, the European regulation (AI act) proposes monitoring throughout the life cycle of the system.

[21] In this regard, Art. 14 of the AI act, in the version amended by the EU Parliament, provide for the following: "High-risk AI systems shall be designed and developed in such a way (…) that they be effectively overseen by natural persons as proportionate to the risks associated with those systems. Natural persons in charge of ensuring human oversight shall have sufficient level of AI literacy in accordance with Article 4b and the necessary support and authority to exercise that function…".

[22] L. d'Avack, *La rivoluzione tecnologica e la nuova era digitale. Problemi etici*, in U. Ruffolo (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Giuffrè, 2020, 25.

[23] V. Rampton, Where telemedicine always falls short, in Science, 2022, 378, 6619, 480.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 147-152
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 10

*Telehealth: A New Relationship with the Territory(ies)?**

Olivier Renaudie
(Full Professor of Public Law at University Paris 1 Panthéon-Sorbonne - Member of the French Association of Health Law (AFDS))

ABSTRACT Starting with some general remarks on telehealth, the article traces backs and highlights some relevant characteristics of the development of the phenomenon in France. In particular, it focuses on the relationship between healthcare services and the local territories, and the possible reshaping thereof that telehealth may contribute to, without however failing to stress the importance not to underestimate the several shortcomings of telehealth, and the reasons why they may ultimately jeopardize telemedicine's many promises of improvements for provision oh healthcare services in the local territories.

1. *Introduction*

Telehealth[1] covers an area that does not lend itself spontaneously to digitalization. Indeed, health care necessarily builds on an almost-tangible relationship of trust between doctor and patient, that by itself implies the doctor's physical presence. One provision of the Code of Medical Ethics prohibits "roving medicine";[2] another specifies that no fee may be charged for advice given by telephone.[3] As one French health minister put it, telehealth "is not a subject like any other, but THE system which, in the years to come, will transform medical practices and even the way we think about health".[4] In the attempt to define the relationship between telehealth and territory(ies), three preliminary remarks should be made.

The first remark concerns to current developments in telehealth in France. These developments are both legal and political. Among the numerous legal developments, the decree of 3 June 2021[5] on telehealth defines the conditions for implementing and supporting remote activities carried out by pharmacists and medical auxiliaries. Equally relevant, the law of 25 November 2021[6] on civil security allows firefighters to carry out telemedical acts as part of their emergency rescue-and-care missions.[7] On the political front, telehealth now permeates every discourse on health. Suffice it to say that telehealth was considered nothing less than one of the pillars of the 2020 conference Ségur de la Santé;[8] and that, in the words of the French Health Minister, telehealth is "an effective solution for accessing healthcare and a powerful ally in overcoming unprecedented challenges, such as the pandemics".[9]

The second remark has to do with the word itself. Before clarifying what telehealth is, it is first necessary to disambiguate what telehealth is not. Indeed, telehealth is not itinerant healthcare, which refers to any movable-health device allowing to provide healthcare services to peoples located in areas with few healthcare professionals. For example, the Region of Normandy and the regional health agency (ARS) have set up "Médicobus", an itinerant consulting room that travels the Normandy department of Orne to reach

* Article submitted to double-blind peer review.

[1] About telehealth, see in particular: O. Babinet and C. Isnard Bagnis, *Et si la télésanté était réponse aux déserts médicaux ?*, in O. Babinet and C. Isnard Bagnis (eds.), *Les déserts médicaux en question(s)*, Hygée. 2021, 147-163; N. Ferraud-Ciandet, *Droit de la télésanté et de la télémédecine*, Paris, Hdf, 2011; P. Lasbordes, *La télésanté: un nouvel atout au service de notre bien-être*, Report submitted to Roselyne Bachelot, Minister of Health and Sport, 2009;

[2] Article 74 of the Code of Medical Ethics (article R 4127-74 of the Public Health Code).

[3] Article 53 of the Code of Medical Ethics (article R 4127-53 of the Public Health Code).

[4] Roselyne Bachelot, opening speech at the symposium on *health information systems*, 6 November 2008.

[5] Decree no. 2021-707 on telehealth.

[6] Law no. 2021-1520 aimed at consolidating our civil security model and enhancing the value of volunteer firefighters and professional firefighters. About it, see O. Renaudie, *La contribution de la loi du 25 novembre 2021 au renouvellement de la sécurité civile*, in *AJCT* 2022, p. 160-165.

[7] Article 3 of Act no. 2021-1520, cited above.

[8] The Ségur de la santé is a consultation of stakeholders in the healthcare system, held at the Ministry of Health from 25 June 2020 to 10 July 2020 (https://solidarites-sante.gouv.fr/IMG/pdf/dossier_de_presse_-_conclusions_segur_de_la_sante.pdf).

[9] Speech given at the launch of "*Mon espace santé*" (https://solidarites-sante.gouv.fr/archives/archives-presse/archives-discours/article/discours-d-olivier-veran-a-la-conference-de-presse-de-lancement-de-mon-espace).

isolated peoples.[10] For all that, it is useful to better clarify the concepts of telemedicine and telehealth.[11] On the one hand, telemedicine and telehealth are similar in that they are both services provided to individuals. On the other hand, telemedicine and telehealth differ in terms of the nature and scope of the services they provide. To put it simply and as stated by the French Public Health Code, telemedicine is "a form of medical practice".[12] Therefore, there can be no telemedicine without doctors. It is useful to briefly recall the definition of medical procedures given by Government Commissioner Fournier in his conclusions on the 1959 *Rouzet* ruling by the Conseil d'Etat,[13] namely "procedures whose performance involves serious complexity and requires a special knowledge acquired through lengthy studies".[14] Following from this definition, such medical procedures can be performed only by doctors or medical auxiliaries supervised by doctors. Differently, telehealth is a much broader concept than telemedicine,[15] as it refers to all health-related activities carried out at distance using information and communication technologies.[16] Such activities may fall under telemedicine; they may also fall under "telecare", as it is known today, i.e. remotely-provided care by a healthcare professional, such as a pharmacist, nurse, or speech therapist.

The third remark relates to what telehealth embodies. Basically, it appears to be a two-faced totem. From the point of view of the healthcare system, telehealth is the epitome of modernisation, able to cure all -and there are many- organisational inefficiencies.[17] From the point of view of the territories -the focus of the present essay- telehealth promises to dissolve the distance between patients and healthcare professionals, and to enable faster and more effective access to care despite geography and physical locations.

This second face of the totem necessarily carries considerations on the relationship between telehealth and territory(ies), and specifically whether telehealth may be leading to a new relationship with the territory(ies). In what follows, the present essay will provide a possible twofold-assessment of the issue. First, it will retrace the context in which telehealth has developed. Secondly, it will identify several shortcomings - that are particularly due to considerations about the territories - of this technology.

2. *The development of telehealth*

In France Telehealth is currently undergoing a rapid development. Indeed, there has been a sharp increase in the number of teleconsultations, especially during the first wave of the health crisis, when the number of teleconsultations increased from 10,000 per week to around one million.[18] Furthermore, there has been an increase also in the variety of patients using telehealth. However, in order to assess the extent of this development, it is necessary to clarify the purposes of telehealth (discussed in section A) and the methods it uses (section B).

2.1. *Objectives*

In order to assess the objectives e-Health pursues, and therefore their connection with the territories, it is important to distinguish between objectives set at the European level, and those defined by French public authorities.

For what concerns the European level, The EU took an early interest in e-Health.[19] In a 2004 Communication titled "eHealth - making

[10] www.normandie.ars.sante.fr/le-medicobus-un-nouveau-dispositif-innovant-de-prise-en-charge-des-soins-non-programmes-dans-lorne.

[11] For further reference, see C. Bourdaire-Mignot, *Téléconsultation: quelles exigences ? Quelles pratiques*, in *RDSS* 2011, pp. 1003-1012 and O. Renaudie, *Télémédecine, télésanté, télésoins: des paroles aux actes*, in *RDSS* 2020, 5-12.

[12] Article L 6316-1 of the French Public Health Code.

[13] CE, 26 June 1959, *Rouzet*, Rec. 405.

[14] *AJDA* 1959, p. 273.

[15] See J.-M. Rolland, *Rapport sur le projet de loi portant réforme de l'hôpital et relatif aux patients, à la santé et aux territoires*, Ass. nat. no. 1441, 5 February 2009,16.

[16] See D. Acker and P. Simon, *La place de la télémédecine dans l'organisation des soins*, Rapport à la direction générale de l'offre de soins, Ministère de la Santé, 2008, 14-16.

[17] About these problems and the possible solutions, see in particular O. Claris, *La gouvernance et la simplification hospitalière*, report, June 2020 (https://solidarites-sante.gouv.fr/IMG/pdf/rapport_claris_version_finale.pdf) and E. Minvielle, *Conditions de travail à l'hôpital : quelles pistes d'amélioration?*, in *Les Tribunes de la santé*, 2021, no. 69, pp. 59-68.

[18] See CNAM, *Améliorer la qualité du système de santé et maîtriser les dépenses. Propositions de l'Assurance Maladie pour 2021*, July 2020 (https://assurance-maladie.ameli.fr/sites/default/files/2020-07_rapport-propositions-pour-2021_assurance-maladie.pdf).

[19] See N. Ferraud-Ciandet, *L'Union européenne et la télésanté*, in *RTDE* 2010, 205-2022 and F. Sauer, *Europe et télésanté*, in *RDSS* 2011, 1029-1036.

healthcare better for European citizens",[20] the Commission adopted an action plan to increase the use of information and communication technologies in the field of health. At the European level, it was precisely this plan that used the term "telemedicine" for the first time, borrowing it from the World Health Organisation. The Union's purposes at the time were - and still are - to guarantee patients' movement among the Member States and to facilitate "cross-border care", i.e. care provided or prescribed by a doctor in Member States other than those where patients were registered. Since then, these two purposes have constantly been reaffirmed by the European institutions, as in the 2008 Communication,[21] in which the Commission urged Member States to "enable better access to telemedicine services by adapting their national legislation".

For what concerns the French level, telehealth developed in three stages. First, in 2004 when telemedicine was cautiously enshrined in law. Indeed, the law of 13 August 2004[22] stated that telemedicine made it possible "inter alia, to carry out medical procedures (...) at a distance, under the control and responsibility of a doctor in contact with the patient by means of communication appropriate to the performance of the medical procedure".[23] However, said poorly-drafted provision,[24] which had been passed at the EU's request, was not followed by any action. Secondly, in 2009, telemedicine was again enshrined in law, but this time more enthusiastically and precisely. Indeed, the law of 21 July 2009,[25] which defined it as "a form of remote medical practice using information and communication technologies"[26] was followed by implementing legislation, in particular the decree of 19 October 2010 on telemedicine.[27] As envisaged at the time, telemedicine purported two main objectives, albeit one more emphasised than the other. First, it meant to improve quality of care,[28] mainly by encouraging cooperation between healthcare professionals and facilitating remote monitoring. For instance, remotely monitoring certain indicators would either stabilize chronic patients or give immediate alert of their worsening health.[29] Secondly, it meant to reduce costs. Indeed, the 2009 Labordes report emphasised that telehealth would "enhance the efficiency of the healthcare system by ensuring optimal use of available resources and skills".[30] More specifically, cost savings would be achieved by curtailing unnecessary patient transfers and emergency-room consultations, and by keeping people in need of assistance at home for longer. Finally, a turning point was achieved with law of 24 July 2019[31] renamed Chapter 6 of the Public Health Code, titled "Telemedicine", which is now called "Telehealth".[32] From then on, Health Ministers have talked about telehealth in different terms, as either an instrument for restructuring care and enabling medical skills to be pooled;[33] or as a tool for "combating medical deserts",[34] making it actually possible to remedy the shortage of practitioners in specific urban and rural areas.[35] For example, telehealth is considered a pathway to compensate the falling access to GPs resulting from the mismatch between supply and demand for care. Therefore, telehealth is permeated with territorial considerations. It is no coincidence that point 24 of the conclusions of Ségur de la Santé states the

[20] European Commission, COM (2004) 356, April 2004.
[21] European Commission, "Telemedicine for the benefit of patients", COM (2008) 699, November 2008.
[22] Law no. 2004-810 on health insurance.
[23] Article 32 of Act no. 2004-810, cited above.
[24] In particular, the use of the expressions "inter alia" and "appropriate means of communication" may be perplexing.
[25] Law no. 2009-879 on hospital reform and patients, health and territories (HPST).
[26] Article 78-I of Act no. 2009-879 (article L 6316-1 of the Public Health Code).
[27] Decree no. 2010-1229 on telemedicine. On this text, see M. Contis, *La télémédecine, nouveaux enjeux, nouvelles perspectives juridiques*, in *RDSS* 2010, pp. 235-246.
[28] On the quality of care, see L. Cluzel, *L'irruption de la qualité dans le domaine sanitaire*, in *RDSS* 2014, p. 1002-1013.
[29] N. Berra, *Opening speech at the scientific day on technological innovations in telehealth, National Assembly*, 13 October 2011 (https://toute-la.veille-acteurs-sante.fr/5564/discours-de-nora-berra-en-ouverture-de-la-journee-scientifique-sur-les-innovations-technologiques-en-telesante-organisee-par-le-carrefour-de-la-telesante-201011-2/).
[30] *Report*, p. 39.
[31] Law no. 2019-774 on the organisation and transformation of the healthcare system.
[32] This is Chapter 6 of Title 1st devoted to emergency medical assistance, permanent care, telehealth and health transport.
[33] https://solidarites-sante.gouv.fr/systeme-de-sante-et-medico-social/masante2022/lutter-contre-les-deserts-medicaux/.
[34] *Ibid.*
[35] See F. Niedercon, *La télémédecine contre les déserts médicaux, un remède mais pas miracle*, in *Les Echos*, 4 April 2022.

need to ensure "the development of telehealth in all regions".[36]

2.2. *Terms and conditions*

Despite telehealth's popularity in recent years, its theoretical classifications and practical functioning remain difficult to grasp and must, therefore, be identified.

As far as theoretical classifications are concerned, article R 6316-1 of the French Health Code refers to four modes of delivery.[37] In "teleconsultation" doctors offer remote consultations to patients, who may be assisted by healthcare professionals at their side. The patients - together with the assisting healthcare professional, if any - provide information and doctors remotely give diagnoses. In "tele-expertise", doctors remotely seek consultations with one or more colleagues. In "remote medical monitoring", doctors remotely monitor and interpret patients' medical parameters. The recording and transmission of data may be automated or carried out by the patients themselves. If necessary, doctors take decisions relating to the patients' care. Finally, in "remote medical assistance" doctors remotely assist other doctors during the performance of procedures, such as surgeries.

Practical functioning can vary. The first possibility for variation relates to the initiative, that can be either private or public, to set up a telehealth service.[38] A second element is material. As pointed out in a recent report by the Senate's delegation for local and regional authorities,[39] telehealth can take two main practical forms. The "telecabin" is an enclosed place with a seat, a screen, online measuring instruments (thermometer, scales, blood pressure monitor, stethoscope, etc), a printer to deliver prescriptions,[40] and all other necessary equipment for teleconsultation allowing patients and healthcare professionals to see and hear each other. The "telehealth practice" is a conventional medical or healthcare practice that meets safety and accessibility standards and is equipped with online measuring instruments.[41] In telemedicine, patients are generally greeted by a nurse who knows how to use such instruments. Unlike telecabins, which are autonomous, telehealth practices require a human presence. However, both have the benefit to be able to provide care to isolated patients.[42] This makes it possible to meet long-term needs, as well as occasional ones. For example, the mayor of Le Favril, in the Eure-et-Loir region, has set up a telecabin to cover for doctors on holiday.[43]

The development of telehealth is undoubtedly reshaping the provision of health in the territories. Being able to dissolve distances, this technology is a valuable tool to fight medical deserts and facilitate isolated patients' access to care. It is not, however a magic wand, and has too a number of shortcomings.

3. *The shortcomings of telehealth*

Since it provides an operative solution to the scarce availability of healthcare services in remote territories, telehealth promises to be both an instrument to modernise healthcare and an effective provision of health services in the territories.[44] However, telehealth is not without faults and its development has proven many of its limitations both technical (section A) and territorial (section B).

3.1. *Technical limitations*

Telehealth is a technological tool. As such, it must overcome a number of technical obstacles in order to meet its objectives and,

[36] https://solidarites-sante.gouv.fr/IMG/pdf/Dossier_de_presse__conclusions_segur_de_la_sante.pdf).

[37] On this subject, see C. Bourdaire-Mignot, *Téléconsultation: quelles exigences? Quelles pratiques, op. cit.*, p. 1003.

[38] See Cour des Comptes, *La télémédecine : une stratégie cohérente à mettre en œuvre* in *Rapport sur l'application des lois de financement de la Sécurité sociale 2017*, September 2017 and C. Meyer-Meuret, *Les enjeux économiques de la télémédecine*, in *RDSS* 2011, 1013-1020.

[39] P. Mouiller and P. Schillinger, *Rapport d'information relatif aux initiatives des territoires en matière d'accès aux soins*, Sénat, no. 63, 14 October 2021, p. 25.

[40] A.-L. Dagnet, *Sub-medicine or real solution, telemedicine practices flourish in medical deserts*, 7 December 2021 (https://www.francetvinfo.fr/replay-radio/le-choix-franceinfo/sous-medecine-ou-vraie-solution-les-cabines-de-teleconsultation-fleurissent-dans-les-deserts-medicaux_4855349.html).

[41] P. Mouiller and P. Schillinger, above-mentioned report, 26.

[42] See R. Le Dourneuf, *Dans l'Essonne, une cabine de télémédecine pour éviter le désert médical*, in *20 minutes*, 20 February 2022 (www.20minutes.fr/paris/3238275-20220220-essonne-cabine-telemedecine-mairie-eviter-desert-medical).

[43] P. Mouiller and P. Schillinger, above-mentioned report, p. 26.

[44] See O. Babinet and C. Isnard Bagnis, *Et si la télésanté était une réponse aux déserts médicaux, op. cit.*, 147-148.

where possible, to reshape the relationship between health-care services and territory(ies). Some shortcomings have already been overcome, while others remain and may slow down its further development.

The now-overcome obstacles were mainly twofold. The first was the personal medical file (DMP), which is a tool for storing personal health data.[45] Instituted by law of 13 August 2004,[46] the personal medical file gave rise to several - mostly technical - troubles before being relaunched by the HPST law of 21 July 2009.[47] Undisputedly, telehealth could not function without the DMP, which enables healthcare professionals to share information regarding a patient.[48] The second obstacle concerned Assurance Maladie's coverage of telehealth services. Indeed, the roll-out of telehealth was met with reluctance by the Social Security system for fear that remote consultations would exponentially increase the number of overall consultations, thus resulting in massive reimbursements requests.[49] These two elements explain why telehealth, and in particular telemedicine, have remained marginal for so long. However, the roll-out of telehealth proved possible to overcome them: firstly, with the creation and widespread use in 2016 of "DMP 2", the shared medical record;[50] and secondly, with the inclusion, in 2017[51] and 2018,[52] of teleconsultations in the healthcare pathway, thus providing a right to reimbursement by the Assurance Maladie.

The obstacles yet to overcome[53] mainly relate to the still-imperfect coverage of the high-speed Internet network which makes it impossible for telehealth to realise its full potential.[54] Truthfully, significant progress has been made. In terms of mobile coverage, the agreement between the French government and telecom operators, known as the "Mobile New Deal",[55] has led to a significant improvement in digital coverage (from 72% to 85%) across the country: including the overseas territories. However, several "white zones", particularly in rural and mountainous areas still remain[56] and prove to be a major obstacle to the effective deployment of telehealth. The problem is exacerbated by the fact that the areas in question often are medical deserts, thus doubling the pain of an already painful conundrum. Furthermore, as the Défenseure des droits pointed out in her February report on the digitalization of public services,[57] some social groups (such as the elderly or people in precarious situations) may have more trouble using digital technologies.[58] For these people, using a telecabin may be far from straightforward. These technical limitations are further aggravated by territorial shortcomings.

3.2. *Territorial shortcomings*

One might be prone to think that telehealth knows no territorial constraint, being able to reach any place free of any physical boundaries and imitations. In reality, this is not at all the case. Indeed, even though telehealth makes it possible to bring together patient and healthcare professionals who are

[45] C. Bourdaire-Mignot, *Le dossier médical personnel : un outil de stockage des données en vue d'une utilisation partagée*, in *RGDM*, 2012, n. 44, 295-311.
[46] Article 3 of Act no. 2004-810, cited above.
[47] Article 50 of the aforementioned law no. 2009-879. The provisions of this article are set out in articles L 1111-14 *et seq*. of the French Public Health Code.
[48] "This tool is essential to the development of [telemedicine] practices, which involve centralising patient health data to which the healthcare professional must be able to access remotely" (C. Bourdaire-Mignot, *op. cit.*, 311).
[49] See C. Meyer-Meuret, *Les enjeux économiques de la télémédecine, op. cit.*, p. 1013 and O. Babinet and C. Isnard Bagnis, in O. Babinet et C. Isnard Bagnis (eds.), *Pourquoi la télémédecine est-elle enfin possible*, *La e-santé en question(s)*, Rennes, Presses de l'EHESP, 2020, 35-48.
[50] Art. 96 of Law 2016-41 of 26 January 2016 on the modernisation of our healthcare system.
[51] Art. 54 of Act no. 2017-1836 of 30 December 2017 on the financing of social security for 2018.
[52] Order of 1er August 2018 approving order no. 6 to the national agreement organising relations between self-employed doctors and the health insurance scheme signed on 25 August 2016 and decree no. 2018-788 of 13 September 2018 relating to the terms and conditions for implementing telemedicine activities.
[53] For an analysis of these obstacles, see P. Mouiller and P. Schillinger, above-mentioned report, pp. 27-28.
[54] See L. de la Raudière and E. Bothorel, *Rapport d'information sur la couverture numérique du territoire*, Assemblée nationale, n. 213, 27 September 2017.
[55] Agreement concluded in January 2018 between the State and the telecommunication operators, negotiated under the aegis of ARCEP, with the aim of closing the territorial digital divide, by accelerating the widespread availability of very high-speed 4G mobile broadband (https://www.arcep.fr/cartes-et-donnees/tableau-de-bord-du-new-deal-mobile.html).
[56] ARCEP, *La couverture des zones peu denses*, 18 March 2022 (https://www.arcep.fr/la-regulation/grands-dossiers-reseaux-mobiles/la-couverture-mobile-en-metropole/la-couverture-des-zones-peu-denses.html).
[57] Défenseur des droits, *Dématérialisation des services publics : trois ans après, où en est-on*, February 2022 (https://www.defenseurdesdroits.fr/fr/rapports/2022/02/rapport-dematerialisation-des-services-publics-trois-ans-apres-ou-en-est-on).
[58] *Report*, p. 14-16.

geographically apart, it is nonetheless a practice firmly rooted in the territories.[59] Indeed, any installation of telecabins or telehealth practices must be preceded by an assessment of the relevant territory. Moreover, careful consideration must also be given to the local authorities involved and to the financial sustainability of the project.

The driving idea should not be to set up a telehealth cabin or practice just anywhere and under any conditions, the assessment of the territory is relevant. In particular, two factors need to be taken into consideration. Firstly, it is important to verify an actual shortage of healthcare in the territory at issue, through consultation of the regional healthcare organisation plan[60] and construction of an effective dialogue between the interested local councils and the ARS. Secondly, it is paramount to identify the living areas covered by the telehealth system, i.e. the share of the population likely to benefit from it.[61] This regional approach is all the more necessary given that some local councils have rushed to set up telehealth practices however unsuited to the territory concerned. This is particularly true of practices set up at the municipal level rather than at inter-municipal level[62] where they would have proven more useful.

The matter of the local entities concerned is a delicate one. In principle, the State has exclusive competence in the field of health.[63] Indeed, article L 1411-1 of the French Public Health Code establishes that "the Nation defines the health policy in order to guarantee everyone the right to health and its protection". It is therefore up to the State to ensure equal access to healthcare and equal distribution of healthcare services throughout the country.[64] This dual objective is in fact one of the main aims of the health policy, which "seeks to ensure (...) the reduction of social and territorial inequalities", as well as "people's effective access to prevention and care".[65] However, the various local authorities are bestowed several subsidiary powers that enable them to act in the field of public health.[66] In this respect, locally-elected representatives may be tempted to respond to their fellow citizens' need to access healthcare in order to compensate the lack of private initiative and the failure of the State. It goes without saying that costs should weigh in on such choice. As the mayor of Laigneville, in the Oise department, pointed out, "telemedicine practice costs the municipality €100,000 a year".[67] It is, therefore, imperative to carefully assess beforehand, both the financial sustainability of the project and the extent of the territories likely concerned.

As these final considerations show, telehealth ought not to be deployed without taking into account the territories, but rather by building on them. In this sense, while telehealth can bring healthcare professionals and patients closer together by dissolving distances, the relationship between healthcare and territory(ies) induced by telehealth is both *revolutionary in* its essence and *very traditional* in its implementation.

[59] See P. Mouiller and P. Schillinger, above-mentioned report, 25-27 and J.-H. Amet-Roze, *La territorialisation de la santé: quand le territoire fait débat*, in *Hérodote*, 2011, n. 143, 13-32.

[60] As stipulated in article L 1434-2 of the Public Health Code, the regional health plan is "drawn up for five years on the basis of an assessment of health, social and medico-social needs and determines, for the whole range of healthcare and health services on offer, including prevention, health promotion and medico-social support, forecasts of developments and operational objectives". About these plans, see B. Apollis and D. Truchet, *Droit de la santé publique*, Dalloz, 11th ed, 2022, pp. 79-80.

[61] On the concept of the catchment area, see C. Aragau, B. Bouleau and C. Mangeney, *Les bassins de vie ont-ils un sens?*, in *Revue d'économie régionale et urbaine*, 2018, 1261-1286.

[62] On the links between intercommunality and health, see for example, P. Allorant, S. Dourmel and F. Eddazi, *Métropolisation et santé à Orléans : quand l'institution métropolitaine ouvre de nouveaux champs d'action*, in *Revue francophone sur la santé et les territoires*, 2022 (https://journals.openedition.org/rfst/1502).

[63] See O. Renaudie, *Eloge de la centralisation sanitaire*, in *AJDA*, 6 July 2020, 1313.

[64] About this dual dimension, see M.-L. Moquet-Anger, *Territoires de santé et égalité des citoyens*, in *RDSS*, 2009, pp. 116-125.

[65] Article L 1411-1 of the French Public Health Code.

[66] About these powers, see P. Villeneuve, *Les compétences sanitaires des collectivités territoriales*, in *RDSS* 2009, 86-97.

[67] Quoted in P. Mouiller and P. Schillinger, above-mentioned report, 25-27.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 153-167
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 11

*Telemedicine: Impact and Perspectives in Healthcare Delivery and Organization of the Italian National Health Service**

Viviana Molaschi
(Associate Tenured Professor of Administrative Law at Polytechnic of Turin, Italy. PoliTO per il Sociale, Osservatorio DIPAB Bicocca)

ABSTRACT The paper discusses the development of telemedicine, the original core and pillar of digital health, in Italy. After having preliminarily framed the topic, also tracing its evolution at European and Italian levels, the analysis devotes ample space to the provisions of the National Recovery and Resilience Plan, for which e-Health and, in particular, telemedicine, represents one of the most important factors for the strengthening of the healthcare system. The reflections are twofold: the effects of remote care on the physician-patient relationship and the impact on service delivery and healthcare organization.

1. *Preliminary considerations*

Scientific-technological innovation affects almost every sphere of contemporary societies, touching also particularly sensitive aspects of our existence such as health.

E-Health is the new frontier both of medicine and healthcare services.[1] This paper will try to offer some insights into telemedicine,[2] one of its most significant forms.

As has been observed by scholars, telemedicine has "relocated" healthcare delivery to a virtual world[3] or, in any case, to a world whose physical location ceases to be relevant in whole or in part. The therapeutic relationship and the treatment, in fact, are characterized by telematic sharing of medical data and remote clinical interventions.

As a consequence of the Covid-19 pandemic, telemedicine has received an extraordinary boost. Hospitals and healthcare facilities were themselves places at risk of contagion, especially for frail individuals (and their families), but also for healthcare personnel: digital healthcare made it possible to provide care while respecting social distancing, thereby containing the spread of the virus.

In addition, coping with the pandemic took a lot of human, instrumental, and organizational resources away from "ordinary" healthcare, resulting in the reduction and suspension of many services. Telemedicine ensured alternative forms of service delivery, albeit with not a few critical issues.

This new way of "practicing medicine" has impacted both the doctor-patient relationship and the delivery and organization of health services, which are now trying to consolidate and systematize the innovations that have had an exceptional impetus in the emergency phase of the pandemic.

This institutional and technical evolutionary effort is also due to the fact that telemedicine is seen as one of the possible responses to the problems that the Italian National Health Service (NHS) has long suffered from, and that Covid-19 has laid bare and exacerbated: the scarcity of economic resources, which had been reduced over the years before the pandemic; the inequalities between the country's various regional healthcare services; criticalities in the healthcare delivery system, such as weakness

* Article submitted to double-blind peer review.

[1] In this regard see A. den Exter, *Editorial: EHealth Law: The Final Frontier?*, in *European Journal of Health Law*, 23, 2016, 227.

[2] Among the earliest scholars of telemedicine, with a specific attention to the public-law perspective, A.L. Tarasco, *La telemedicina per lo sviluppo della sanità del Mezzogiorno: una introduzione giuridica*, in *Rivista giuridica del Mezzogiorno*, 2010, 4, 1387. For an overview of the challenges, problems and opportunities related to this field see, recently, A. Mazza Laboccetta, *Telemedicina: sfide, problemi, opportunità*, in *federalismi.it*, 22, 2023, 135. On telemedicine as a new (and problematic) frontier of the right to health see L. Ferraro, *La telemedicina quale nuova (e problematica) frontiera del diritto alla salute*, in *Il diritto dell'informazione e dell'informatica*, 2022, 837.

[3] On this kind of "relocation" of healthcare services see A. Mazza Laboccetta, *Telemedicina: sfide, problemi, opportunità*, 137.

of the territorial services, which burdened hospitals with pressure that proved unbearable during the health emergency. As to the latter, the Covid emergency has highlighted the harmful consequences of some regions' decisions to reduce the network of home services, in connection with the downsizing of territorial ones, including those provided by general practitioners. This is one of the reasons behind the heavy impact of the pandemic on the hospital system, which risked collapse.[4]

Starting with framing the relevant context - what telemedicine is, what evolution it has had at the European and national level - the article will discuss in particular the reforms and interventions provided by the National Recovery and Resilience Plan (NRRP) of 2021 and its subsequent implementation.

Concluding remarks will address, firstly, some issues relating to how the development of telemedicine affects the physician-patient relationship and the role of the patient with respect to his or her own health.

Excluded from the discussion are profiles such as data protection[5] and the liability regime,[6] which are also part of the complex and articulated law, in the making, for telemedicine.[7]

The paper, moreover, will investigate the effects of telemedicine on healthcare supply and on the guarantees of care provided by the healthcare system, while also offering remarks on some issues relating to healthcare organization.

2. *Telemedicine: development and definitions*

By digital health (e-Health) is meant the use of information-and-communication-technologies (ICTs) tools and services in healthcare in order to support and improve prevention, diagnosis and treatment of diseases, monitoring and management of health as well as the lifestyles affecting it.[8]

It is therefore a heterogeneous set of instruments, partly because of the fluidity and pervasiveness of the technologies that make its "substrate". Indeed, scholars have pointed out that "giving an unambiguous definition of digital health constitutes a balancing act between oversimplification and incompleteness".[9]

Political-administrative processes that relate to e-Health should also be included in the definition.[10]

Telemedicine, which is, in a nutshell, remote diagnosis, treatment and monitoring of patients, is the first antecedent and original core of e-Health. In fact, its origins go back in time.[11]

Among the most cited examples is that of electrocardiographic consultations that the inventor of electrocardiography, physiologist Willem Einthoven, carried out over the telephone around 1906. Despite the conspicuous limitations of the technologies of the time, the idea of telemedicine was already conceived.

The first remote transmission of radiological images happened for the first time in 1950, in Pennsylvania. In 1959, the Nebraska Psychiatric Institute and Norfolk State Hospital developed the first interactive teleconsultation service. Finally, in the late 1960s, Boston International Airport and

[4] On these issues, one may refer to V. Molaschi, *Integrazione socio-sanitaria e COVID-19: alcuni spunti di riflessione*, in *Il Piemonte delle Autonomie*, 2020, 2.

[5] On the protection of privacy in the field of telemedicine see, *ex multis*, F.G. Cuttaia, *Lo sviluppo della telemedicina e i profili di tutela della privacy ad essa connessi*, in *Studi parlamentari e di politica costituzionale*, 2018, 201-202, 27. With special reference to data protection in healthcare data bases see M. Campagna, *Il regolamento europeo 679/2016 e l'utilizzo delle banche dati in sanità*, in A. Monica and G. Balduzzi (eds.), *Governare il cambiamento istituzionale e organizzativo nelle amministrazioni europee*, Pavia, Pavia University Press, 2019, 59 *et seq*. More in general, on data protection in the new world of artificial intelligence see F. Pizzetti, *Intelligenza artificiale, protezione dei dati personali e regolazione*, Turin, Giappichelli, 2018.

[6] For some issues of professional liability arising from the provision of services remotely see F. Aperio Bella, *The Role of Law in Preventing "Remote" Defensive Medicine: Challenges and Perspectives in the Use of Telemedicine*, in *federalismi.it*, 1, 2023, 305.

[7] In this regard see C. Botrugno, *Un diritto per la telemedicina: analisi di un complesso normativo in formazione*, in *Politica del diritto*, 2014, 639.

[8] For this definition see N. Matteucci and N. Marcatili, *E-health ed evoluzione dei sistemi sanitari. Un'analisi empirica sull'Europa*, in G. Vicarelli and M. Bronzini (eds.), *Sanità digitale. Riflessioni teoriche ed esperienze applicative*, Bologna, il Mulino, 2019, 51.

[9] In these terms see M. Campagna, *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19*, in *Corti supreme e salute*, 2020, 601.

[10] See again N. Matteucci and N. Marcatili, *E-health ed evoluzione dei sistemi sanitari. Un'analisi empirica sull'Europa*, cit., 51.

[11] For a brief history of telemedicine, with a description of the first experiments and experiences, see C. Botrugno, *Telemedicina e trasformazione dei sistemi sanitari. Un'indagine di bioetica*, Roma, Aracne, 2018, 15.

Massachusetts General Hospital pioneered a teledermatology project involving the transmission of gray-scale images.

Last but not least, one must not forget the experiments that the National Aeronautics and Space Administration (N.A.S.A.) carried out, at the turn of the 1960s, to provide medical care to personnel on orbital missions and to monitor the physical condition of astronauts away from Earth.

The introduction of telemedicine went through ups and downs, including moments of failure. This first season of experimentation continued until the late 1980s, but did not yield the desired results due to the poor quality of the audio and video systems and the elementary operation of the transmission devices. For these reasons, as well as for issues of cost-effectiveness, telemedicine remained relegated to extraordinary interventions and failed to make its way into ordinary medical practice.

Telemedicine has developed mainly since the 1990s, thanks to the improvement of audio-video transmission instruments and the decreasing cost of ICTs.

At this time, particularly in the United States and Canada, there was a change in perspective. Medical trials in the field acknowledged the idea that telemedicine was no longer merely an extraordinary measure, but also a tool for addressing structural deficiencies in health services in specific territories, such as rural areas.

In the 1990s, remote medical intervention underwent conceptualization, and various notions of telemedicine were elaborated, including the WHO's definition of telemedicine (1997). According to it, telemedicine is "the delivery of healthcare services, where distance is a critical factor, by all healthcare professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interest of advancing the health of individuals and their communities".[12]

In Italy, the "National Guidelines" ("Telemedicina – Linee di indirizzo nazionali"), adopted through an Agreement stipulated in the State-Regions Permanent Conference on February 20, 2014, provided one of the first -and still- relevant definition of telemedicine: telemedicine is "a mode of delivery of healthcare services, through the use of innovative technologies, in particular Information and Communication Technologies (ICT), in situations where the health professional and the patient (or two professionals) are not in the same location". It implies "the secure transmission of medical information and data in the form of text, sound, images, or other forms necessary for the prevention, diagnosis, treatment, and subsequent follow-up of patients". The document also clarifies that telemedicine "does not represent a separate medical specialty": telemedicine services "should be equated with any diagnostic/therapeutic health service".

The 2014 Guidelines set the course for subsequent definitions.

According to the "National Directions for the Delivery of Telemedicine Services" ("Indicazioni nazionali per l'erogazione di prestazioni in telemedicina") of 2020, telemedicine "represents an innovative approach to healthcare practice by enabling the delivery of services at a distance through the use of digital devices, software, and telecommunication networks". Thanks to it, "it is possible to ensure the use of health services without the patient or caregiver having to travel to healthcare facilities".

The National Directions bear a classification of telemedicine services on the basis of their appropriateness, which outlines an interesting articulation of their relationship with traditional services. Four types of services are provided: services that can be assimilated to any traditional diagnostic and/or therapeutic healthcare service, representing an alternative delivery; services that cannot replace the traditional healthcare services but rather support them by making them more accessible and/or increasing their efficiency and distributive equity; services that supplement the traditional ones in varying proportions by making them more effective and more capable of adapting dynamically to changes in patients' care needs; services that are capable of completely replacing the traditional healthcare services, representing new diagnostic and/or therapeutic methods and/or techniques and implementing new care

[12] WHO, *A health telematics policy in support of WHO's Health-For-All strategy for global health development. Report of the WHO group consultation on health telematics*, 11-16 December 1997, Geneva, Switzerland.

practices useful to patients.

A more recent definition can be found in Ministerial decree 77 of 23 May 2022, "Regulation defining standard models for the development of territorial care of the National Health Service" ("Regolamento recante la definizione di modelli standard per lo sviluppo dell'assistenza territoriale del Servizio Sanitario nazionale"), according to which telemedicine is "a mode of delivery of sociomedical health-care services and services having health relevance at a distance, enabled by information and communication technologies, and used by a health professional to provide healthcare services to the patients (telemedicine health professional - patient) or consulting with and support services to other health professionals (telemedicine health professional - health professional)". Interestingly, according to this definition, telemedicine encompasses not only healthcare, but also integrated healthcare and social services.

3. *Brief references to the role played by the European Union in the development of telemedicine*

The European Union has played a significant role in the digitization of health services and, specifically, in the development of telemedicine. However, since this paper is focused on its evolution at the national level, suffice it to recall just a few key moments of the European push in this direction.

As scholars have duly noted, the European Union's attention to telemedicine traces back to three reasons of interest that have shaped its development:[13] reducing the economic burden of public healthcare, due primarily to chronic-degenerative diseases, which become more and more common with ever-lengthening life expectancy; fostering EU health mobility and allowing EU citizens to access healthcare services in any Member State; promoting technological innovation in e-Health to foster capital and economic growth. In this framework, the Covid-19 pandemic occurred and gave strong impulse to e-Health, including remote care, in the healthcare systems of Member Countries.

Given the States' competences on health,[14] the EU intervention has mainly consisted of *soft law*. The Union and, specifically, the Commission works on coordinating and integrating services, with the aim of creating an efficient European health governance[15] able to address health emergencies.

These efforts urge States in the direction of greater legal clarity to give institutions, practitioners, and patients confidence in the digital health system; encourage good practices and promote their spreading. Crucial in this framework is achieving interoperability across different health systems.

In a Communication of 2004,[16] the European Commission identified e-Health as an important tool for improving the full range of functions of the health sector: prevention, diagnosis, treatment, health surveillance, and lifestyle management. The EU has envisioned a European e-Health space and defined actions to be taken for its realization. And telemedicine was also part of this framework.

The European Commission specifically tackled the issue in 2008, with a Communication, which (already in the title: "telemedicine for the benefit of patients, healthcare systems and society") revealed high expectations.[17] The Union aimed at supporting and encouraging Member States by identifying and helping to overcome the main barriers to the wider use of telemedicine and by providing elements to build trust and foster

[13] For this analysis see A. Mazza Laboccetta, *Telemedicina: sfide, problemi, opportunità*, 143. On the European policies on e-Health see E. di Carpegna Brivio, *e-Health as a multilevel public policy*, in *European Review of Digital Administration & Law*, vol. 4, issue 1, 2023, 7.

[14] EU and Member States competences on health are established by art. 168(7) of the Treaty on the Functioning of the European Union. On the dynamic relationship between the European and the national competences see M. Guy, *Towards a European Health Union: What Role for Member States*, in *European Journal of Risk Regulation*, 4, 2020, 757 et seq.

[15] The topic of digital healthcare governance has recently been tackled, including with insights on its multilevel articulation, by F. Cimbali, *La governance della sanità digitale*, Padova, Wolters Kluwer/Cedam, 2023. More in general, see E. Mossialos, G. Permanand, R. Baeten and T. Hervey (eds.), *Health Systems Governance in Europe. The Role of European Union Law and Policy*, European Observatory on Heath Systems and Policies, Cambridge, Cambridge University Press, 2010.

[16] COM (2004) 356 final, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area.

[17] COM (2008) 689 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society.

its acceptance.

Also significant was the Digital European Agenda of 2010,[18] in particular Key Action 13, which underlined the need for useful pilot actions to provide European citizens with secure access to their personal-health data and to widely deploy, as far as relevant here, telemedicine services, a goal to be achieved, according to this document, by 2020.

Telemedicine facilitates cross-border healthcare: from this point of view, the evolution of the issue has been marked by the EU's Cross-Border Healthcare Directive, passed in 2011,[19] aimed at ensuring that patients would be able to access safe and high-quality healthcare services (including telemedicine services) across the EU. The Directive, transposed into Italian law with Legislative Decree n. 38 of March 2014, gives EU citizens right to receive healthcare services in Member States other than their own, and to obtain reimbursement for the costs incurred.

In 2012, the Commission outlined the eHealth Action Plan 2012-2020,[20] which shows great awareness of the market potential of e-Health, including telemedicine, in particular as a tool for managing chronic diseases. Among others, it sets the goals to enhance interoperability of e-Health systems across Member States and improve exchange of patient information.

Institutions and health professionals' need for shared guidance led to the 2013 Telehealth Service Code of Practice for Europe, focused on collecting and systematizing best practices related to the use of telemedicine services, and on guaranteeing quality standards for the beneficiaries.

Also worth mentioning is the 2018 Communication on the Digital Transformation of Health,[21] dealing with the need to provide reforms and innovative solutions to the health sector, in order to achieve more resilient, accessible, and effective welfare systems, able to provide quality care to European citizens. The Commission sees digital health and care solutions as means to enhance the well-being of millions of citizens. In fact, according to the Communication, such tools bring numerous benefits: supporting continuity of care across borders; promoting health and preventing disease, including in the workplace; supporting the reform of health systems and their transition to new care models, centred on people's necessities; enabling a shift from hospital-centred systems to more community-based and integrated care structures. The latter is one of the main reasons for Italy's expansion of telemedicine.

As anticipated, the pandemic has brought health to the center of European policies, despite the noticeable (and unchanged) limits of the Union's competence in the field. In the words of Ursula von der Leyen, President of the European Commission, speaking at the World Health Summit (25 October 2020), "We cannot wait for the end of the pandemic to repair and prepare for the future. We will build the foundations of a stronger European Health Union in which 27 Countries work together to detect, prepare and respond collectively".

In order to face the Covid-19 health crisis, the Union adopted the EU4Health programme (2021-2027), established by EU regulation 2021(522).[22] The programme, supported by an unprecedented financial effort in the health sector,[23] has four general objectives (art. 3), which can be summarized as follows: improving and fostering health in the Union; protecting people from serious cross-border threats to health; improving the availability, accessibility and affordability of medical products, medical devices and crisis-relevant products in the Union; strengthening health systems by improving their resilience and

[18] COM(2010)245 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe.

[19] Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare.

[20] COM(2012) 736 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century.

[21] COM(2018) 233 final, Communication from the Commission to the European Parliament, 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.

[22] Regulation (EU) 2021/522 of the European Parliament and of the Council of 24 March 2021 establishing a Programme for the Union's action in the field of health ('EU4Health Programme') for the period 2021-2027, and repealing Regulation (EU) No 282/2014.

[23] The investment is € 5.3 billion budget during the 2021-27 period.

resource efficiency.

General objectives are articulated into specific ones, which also devote attention to e-Health and to the digital transformation of healthcare systems, especially as far as the creation of a European health-data space is concerned (art. 4, point f). The "possible eligible actions" referred to e-Health are: "Supporting the optimal use of telemedicine and telehealth, including through satellite communication for remote areas, fostering digitally-driven organisational innovation in healthcare facilities and promoting digital tools to support citizen empowerment and patient-centred care" (Annex I, point 6, lett. d); "Actions to support e-Health, such as the transition to telemedicine and at-home administration of medication" (Annex I, point 6, lett. i).

With Next Generation EU and, in particular, through the Recovery and Resilience Facility (RRF),[24] the EU is pursuing two fundamental goals: mitigating the social and economic impact of the pandemic; building a greener and more digital Europe.[25] Thanks to this instrument, EU Countries receive financing on the basis of their national recovery and resilience plans,[26] which outline the reforms and investments they will implement by the end of 2026.[27]

The RRP and the follow-up measures take into account the implementation of the European Pillar of Social Rights.[28] "Health, and economic, social and institutional resilience, with the aim of, *inter alia*, increasing crisis preparedness and crisis response capacity" is also one of its columns.

The goal of modernizing and strengthening healthcare services is a priority for the Italian NRRP. As will be illustrated in this paper, in Italy e-Health and, in particular, telemedicine are an essential tool for the transformation of the NHS.

4. *Evolution of telemedicine in the Italian NHS: a general overview*

In order to both better frame the meaning of telemedicine in the Italian NHS, and to provide some concluding remarks it is important to recall some of the stages that have marked the "evolution" of telemedicine in the Country.

First of all, the aforementioned National Guidelines of 2014 gave an initial definition. The purpose of the Guidelines was to provide, after a season of multiple experimental initiatives in the territory, "the unified national reference for the implementation of telemedicine services", with a view to move from an experimental to a structured logic. The document thus aimed to provide a shared governance model for the various actions, and to harmonize guidelines and application models to the benefit of services' interoperability.

The Guidelines provided a classification of telemedicine services,[29] later taken on, specified and supplemented by the subsequent National Directions for the Delivery of Telemedicine Services of 2020 (Indicazioni nazionali per l'erogazione di prestazioni in telemedicina),[30] whose contents will be explained shortly.

The Guidelines of 2014 gave important guidance on the organization of telemedicine services, information and training, integration of telemedicine into the NHS, and so on.

Another important step toward the

[24] Regulation (EU) 2021/241 of the European Parliament and of the Council of 12 February 2021 establishing the Recovery and Resilience Facility.

[25] The amount of resources put in place to boost growth, investment and reforms amounts to 750 billion euros, of which more than half, 390 billion, are grants.

[26] For an overview of the various Member States' recovery and resilience plans see the reports published on the *Italian Labour Law e-Journal*, 1s/2022.

[27] The plans had to allocate at least 37% of their budget to green measures and 20% to digital ones.

[28] See the European Parliament Resolution of 19 January 2017 on a European Pillar of Social Rights (2016/2095(INI)), and COM(2021) 102 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Pillar of Social Rights Action Plan.

[29] According to the Guidelines of 2014, the main branches of telemedicine are:
i) Specialist telemedicine, which is divided into:
- Televisit: health act in which the physician interacts remotely with the patient (perhaps with the support of a care-giver),
- Teleconsultation: remote consulting activity between physicians, without the physical presence of the patient, about diagnosis, choice of appropriate treatment,
- Telecooperation health care: an act consisting of assistance provided by one physician or other health care provider to another physician or health care provider (the term is also used for counseling provided to emergency responders);
(ii) Telehealth: a telemedicine activity carried out at the primary care level. Among the activities carried out under telehealth is telemonitoring.
(iii) Telehealth: a social welfare system for taking care of the elderly or frail person at home.

[30] For example, according to the Directions of 2020, telemedicine also includes telereferral and telephone triage.

development of telemedicine in Italy was taken with the 2016 "National Plan for Chronic Care" ("Piano nazionale delle cronicità"), the outcome of an Agreement sanctioned in the State-Regions Conference on September 15, 2016, in which telemedicine, together with teleassistance, were seen as instruments to facilitate management of patients' homecare, including chronic ones.

However, the European Commission's "Report State of Health in the EU - Italy. Health Profile of 2019"[31] revealed that the digitization of the NHS had advanced at different pace across Italian regions and that since the approval of the 2014 Guidelines "little" had been done to implement the various opportunities.

The insufficient progress of digital health and, specifically, telemedicine was made manifest during the Covid-19 pandemic, which called attention to the need for adequate territorial healthcare and a strong hospital-territory relationship, and highlighted the importance of remote-care models (and of their uniformity). During the health emergency, the NHS was called upon to provide services to an unprecedented number of persons obliged to go into quarantine or "trust" isolation. It was necessary to counter the spread of Covid-19 and to ensure, as far as possible, the continuity of care and assistance to which people are entitled. Moreover, people who were isolated in their own homes as a result of necessary social-distancing regulations could also need care and assistance.

Very significant in the evolution of telemedicine are the 2020 Reports of the Istituto Superiore di Sanità (ISS), that is the main center for research, control and technical-scientific advice on public health in Italy, which provided *interim* directions for telemedicine healthcare services to both adult patients and pediatric patients in their early childhood and developmental age.[32] These documents supported the implementation of remote services during the Covid-19 emergency, offering guidance, identifying operational issues and proposing solutions that were evidence-based and, at the same time, also easily employable in practice.

2020 is also the year of the National Directions for the Delivery of Telemedicine Services (Indicazioni nazionali per l'erogazione di prestazioni in telemedicina), adopted by a State-Regions Conference Agreement on December 17, 2020, which marked the "full-fledged" entry of telemedicine into the NHS,[33] setting rules for the provision of remote healthcare services as to payment, prescriptions, bookings, reporting.

Concerning payments, the Agreement has established that the national/regional regulatory framework on access to the various essential levels of care granted by the NHS, together with the remuneration/tariff system in force for their supply, including the rules for any cost-sharing, also applies to all health services provided remotely.

On November 18, 2021 an Agreement in the State-Regions Conference adopted the "Directions for the provision of telerehabilitation services by the health professions" ("Indicazioni nazionali per l'erogazione di prestazioni e servizi di teleriabilitazione da parte delle professioni sanitarie"). This document has provided uniform directions for the entire Italian healthcare system and especially in the matters of telerehabilitation services by health professions, physicians and psychologists (collectively referred to as "health professionals"), alone or in combination with one another and with other health services.

As already said, the pandemic has marked an acceleration in the evolution of telemedicine, whose development has been boosted by the National Recovery and Resilience Plan (NRRP) of 2021.[34] The Plan defines goals, reforms and investments that Italy intends to carry out through Next

[31] See the OECD/European Observatory on Health Systems and Policies, *Italy: Country Health Profile 2019*, State of Health in the EU, OECD Publishing, Paris/European Observatory on Health Systems and Policies, Brussels, 2019.

[32] See the ISS Covid 19 Report n. 12/2020 of April 13, 2020, "*Interim* provisions for telemedicine healthcare services during the Covid-19 health emergency", and the ISS Covid-19 Report n. 60/2020 of October 10, 2020, "*Interim* provisions for telemedicine healthcare services in pediatrics during and beyond the Covid-19 pandemic".

[33] For this observation see L. Fassari, *La telemedicina entra a pieno titolo nel Ssn. Ecco le linee guida del Ministero con le regole per visite, consulti, referti e teleassistenza* (15 December 2020), in *quotidianosanità.it*.

[34] For an analysis of the NRRP provisions on telemedicine see N. Posteraro, *La telemedicina*, in V. Bontempi (ed.), *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, Roma, Roma TrE-Press, 2022, 201.

Generation EU funds to mitigate the Covid-19 socio-economic impact and to make Italy a greener, more digitalized and more inclusive Country, with a dynamic and stronger economy. It also aims at enhancing the national health welfare through policies of reform and massive economic contribution after years of defunding.[35] The Plan, in fact, has a specific Mission, N. 6, devoted to "Health".[36]

As the NRRP itself points out, the pandemic has highlighted that health is an area that requires "significant digital upgrading".[37] Digital health is a "cross-cutting" area of action that characterizes both of the components of Mission 6 of the Plan, entitled "Health",[38] which are 1) "Proximity networks, facilities and telemedicine for territorial care" (M6C1) and 2) "Innovation, research and digitalization of the National Health Service" (M6C2).

The first component aims at strengthening healthcare services provided in the territory through the enhancement and creation of territorial facilities and units (such as the Community Homes and Community Hospitals), the reinforcement of home care and more effective integration with all social and health services. It also deals, as the title suggests, with telemedicine, whose implementation is essential for the realization of the other NHS priorities.

The goals of the measures under the second component are the renovation and modernization of existing technological and digital facilities; the completion and dissemination of the electronic health record; the improvement of the capacity for the delivery and monitoring of the essential levels of healthcare (the so called, in Italian, "Lea sanitari"[39]) through more effective information systems. As to the latter, the NRRP action is aimed at enhancing the Nuovo Sistema Informativo Sanitario (NSIS), a new health information system consisting of a technological infrastructure managed by the Ministry of Health, which is also conceived as a support for the policy and planning functions relating to health services.

Significant resources are also allocated by the Plan to scientific research and to foster technology transfer, as well as to strengthen the skills and human capital of the NHS, including training of health staff.

The second component of the NRRP also returns to deal with telemedicine through the funding of the National Platform of Telemedicine.

The next paragraph is devoted to analyzing in detail the provisions regarding telemedicine. Before explaining them, it must be remembered that, for "Health", as for the other Missions of the Plan, the components of the State action bear both funding aimed at specific interventions and reforms that are needed for the progress of the Country.

4.1. *In particular: reforms and interventions on telemedicine provided by the National Recovery and Resilience Plan and by subsequent regulations*

The general goals listed in Mission 6 on "Health" by the NRRP with respect to telemedicine are: a) developing telemedicine and overcoming the fragmentation and lack of homogeneity of health services offered in the territory; b) developing advanced telemedicine solutions to support home care.

As seen, telemedicine is addressed in both of the components of the Mission under analysis.

The first one, "Proximity networks, facilities and telemedicine for territorial healthcare" (M6C1), makes evident from its very title that telemedicine is the "backbone of strengthening territorial healthcare":[40] telemedicine, in fact, shifts the center of gravity of healthcare intervention from the hospital to patients' homes.[41]

[35] On the Plan's push in the direction of revitalizing national health welfare see L. Chieffi, *Una nuova stagione per I diritti sociali? La spinta offerta dal* Recovery Fund *per il rilancio dei welfare sanitari*, in *BioLaw Journal – Rivista di BioDiritto*, 2021, 4, 3. More specifically, on the reforms and interventions of the Plan in the healthcare field see A. Pioggia, *La sanità nel Piano Nazionale di Ripresa e Resilienza,* in *Giornale di diritto amministrativo*, 2022, 2, 165.

[36] The Plan is articulated into six Missions: Digitization, Innovation, Competitiveness, Culture and Tourism; Green Revolution and Ecological Transition; Infrastructure for Sustainable Mobility; Education and Research; Inclusion and Cohesion; and Health. Every Mission is made up of various components.

[37] See page 18 of the NRRP.

[38] For the provisions on "Health" see pages 225 et seq. of the NRRP.

[39] On the meaning of the "Lea sanitari" within the Italian NHS see section 5.2.

[40] See page 18 of the NRRP.

[41] For this comment see C. Botrugno, *La diffusione dei modelli di cura a distanza: verso un "diritto alla telesalute"?,* in *BioLaw Journal – Rivista di BioDiritto*, 2014, 1, 164.

In this context Reform 1, entitled "Proximity networks, facilities and telemedicine for territorial healthcare, and national health, environment and climate network",[42] has provided for the "definition of homogeneous structural, organizational and technological standards for territorial healthcare and the identification of the facilities deputed to it", a provision that has been implemented by the aforementioned Ministerial decree No. 77 of May 23, 2022. In this decree, telemedicine is integrated into the new design of the territorial healthcare system.

Another important regulation in which telemedicine fits into the context of the interventions envisaged in the NRRP for the reform of territorial care is the Ministerial decree of April 29, 2022 ("Approvazione delle linee guida organizzative contenenti il 'Modello digitale per l'attuazione dell'assistenza domiciliare'"), that approves the organizational guidelines containing the "Digital model for the implementation of home care". The guidelines define a reference model for the realization and development of the various telemedicine services in the home setting, through the identification of innovative processes for taking care of the patient at home and the definition of the related operational aspects and the enhancement of multiprofessional and multidisciplinary collaboration between different professionals.

Finally, with the decree of September 21, 2022 ("Approvazione delle linee guida per i servizi di telemedicina - Requisiti funzionali e livelli di servizio"), the Ministry of Health has approved guidelines for the functional requirements and service levels of telemedicine. The guidelines lay down technical and service standards for telemedicine healthcare delivery to be widespread and homogeneous across the territory.

As to interventions, the NRRP considers home care and telemedicine in the same investment line (Investment 1.2: "Home as the first place of care and telemedicine"). This makes it again clear that the Plan focuses on telemedicine as a tool for enhancing home care. The use of telemedicine enables continuity of care and is functional to supporting patients with chronic diseases.[43]

Telemedicine is conceived as a means that can, firstly, contribute to the reduction of geographic and territorial gaps through the harmonization of standards of care provided by technology; secondly, ensure a better "care experience" for the assisted; thirdly, improve the efficiency levels of regional health systems through the promotion of home care and remote monitoring protocols.

The NRRP intervention takes the form of funding for telemedicine projects proposed by regions. There are no limits as to what clinical areas can be covered. A wide range of functionalities along the entire pathway of prevention and care can be promoted: tele-care, tele-consultation, tele-monitoring and tele-referral.[44]

Among the conditions set for funding regional projects is their integration with the electronic health record: this provision builds a "bridge" between telemedicine and the other pillar of digital health in the NRRP.[45]

In addition, projects have to achieve quantitative performance targets related to the main goals of telemedicine and the National Health System, as well as to ensure that their development results in the effective harmonization of health services. Moreover, the NRRP clarifies that projects that insist on multiple regions, leverage existing successful experiences, and seek to build true telemedicine platforms that are easily "scalable" will be privileged.

Telemedicine is also addressed in the second component of the NRRP Mission on

[42] According to Reform 1, the NRRP also aims to implement a new institutional arrangement for health, environmental and climate prevention, in line with the "One-Health" approach. The "One-Health" philosophy is a healthcare model, based on the recognition that human health, animal health and ecosystem health are inextricably connected.

[43] The Decree of the Ministry of Economy and Finance of August 6, 2021 has provided within this investment a specific sub-investment 1.2.3, "Telemedicine for better support of chronic patients". It consists of one billion euro.

[44] For the definition of these sub-categories within telemedicine services see the Ministry of Health's 2014 Guidelines and the subsequent 2020 National Directions.

[45] For a comprehensive analysis of the development of the electronic health record in Italy see N. Posteraro and S. Corso, *The Italian Electronic Health Record*, published in this issue of *Erdal*; Id., *Il fascicolo sanitario elettronico*, in V. Bontempi (ed.), *Lo Stato digitale nel Piano Nazionale di Ripresa e Resilienza*, 187; Id., *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *federalismi.it*, 2021, 26,189.

"Health", regarding "Innovation, research and digitalization of the National Health Service" (M6C2), which provides for the creation of a National Telemedicine Platform where demand and supply of telemedicine services provided by accredited entities can meet.[46] The purpose of the Platform is to promote common standards for telemedicine services developed by the regions in order to allow their interoperability and to improve their quality. The initiative aims at facing the challenge of overcoming inequalities in the provision of services and care among different territorial areas.

The entity responsible for the design, implementation and management of the enabling services of the National Telemedicine Platform has been identified as the Agenzia nazionale per i servizi sanitari regionali (Agenas), that is the National Agency for Regional Health Services. According to the Report on the status of implementation of the National Recovery and Resilience Plan of May 31, 2023, the procedure carried out by Agenas for selecting proposals for Public Private Partnership was concluded and a contract was signed.[47]

5. *Concluding remarks: some considerations on the impact of telemedicine on the doctor-patient relationship*

Digital healthcare affects the doctor-patient relationship in many ways.[48] The ambivalence that characterizes all technological progress[49] also arises with respect to this issue.

Telemedicine offers the possibility of treatment from afar, without being present, which allows for patient care anytime and in any place, but sacrifices the value and meaning of the in-person interaction, itself having therapeutic relevance.[50]

As early as 2006, the National Bioethics Committee expressed concern about the "loss of full communication" between the physician and the patient and, in particular, the "loss of that group of objective signs (general look of the patient, posture, deambulation, objective examination by inspection, palpitation, auscultation, percussion, etc.) which, together with elements of emotive perception, guide the diagnostic process in the context of the correct medical semeiotic on the physicality of the person".[51]

The National Guidelines of 2014 have clarified that telemedicine does not replace traditional healthcare in the personal doctor-patient relation, but rather complements it to potentially improve effectiveness, efficiency and appropriateness. However, the risks of "dehumanization" has been nevertheless stressed by several authors. Scholars have highlighted a potential contradiction between the trend toward a more humane, "dialogic" medicine, which is embodied, for instance, in the legislation on informed consent,[52] and the "robot-doctor".[53]

Generally, when speaking about privacy, one thinks of issues concerning data protection. In the field of telemedicine, management of health data, which is necessary to make healthcare delivery itself possible, is particularly complex because of the large amount of data transmitted (through texts, images, audio, video, and so on) and the variety of subjects that can potentially access them.

[46] The above-mentioned sub-investment 1.2.3, "Telemedicine for better support of chronic patients", consisting of 1 billion euro, has been allocated by the decree of the Ministry of health of April 1, 2022, in two lines: 250 million for the implementation of the National Telemedicine Platform and 750 million for regional services.

[47] On February 15, 2023, a contract was signed between AGENAS and the Temporary Business Grouping (RTI) Engineering Ingegneria Informatica S.p.A. and Almaviva S.p.A. for the concession awarding of the "Design, Implementation and Management of the Enabling Services of the PNRR National Telemedicine Platform".

[48] On the metamorphosis of the doctor-patient relationship resulting from the use of telemedicine see C. Casonato, *Telemedicina. Vantaggi e rischi della telemedicina assistita da intelligenza artificiale*, in E. Rigo (a cura di), *Per una ragione artificiale. In dialogo con Lorenzo d'Avack su Costituzione, ordine giuridico e biodiritto*, Roma, Roma TrE-Press, 2023, 219, and C. Botrugno, *Telemedicina e trasformazione dei sistemi sanitari. Un'indagine di bioetica*, 133.

[49] On such ambivalence see A. Simoncini, *Sovranità e potere nell'era digitale*, in T.E. Frosini, O. Pollicino, E. Apa and M. Bassini (eds.), *Diritti e libertà in Internet*, Milan, Mondadori education, 2017, 26.

[50] See F.E. Brozzetti, G.M. Cannella and A. Randazzo, *Telemedicina, teleassistenza e intelligenza artificiale in un sistema socio-sanitario di prossimità: nuovi paradigmi etico-giuridici*, in *Rapporto DIPAB 2022*, *L'integrazione socio-sanitaria e il diritto delle regioni*, Turin, Giappichelli, 2022, 277.

[51] See the document of the National Bioethics Committee, *Ethics, health and new information technologies*, 21 April 2006, 49-50.

[52] In Italy, the matter is governed by Law 217 of 22 December 2019, on informed consent and advance treatment directives.

[53] See R. Balduzzi, *Cinque cose da fare (e da non fare) in sanità nella (lunga e faticosa) transizione verso il post-pandemia*, in *Corti supreme e salute*, 2020, 353.

However, such issues are not discussed in these concluding remarks, and the impact of technologies on privacy is considered from another perspective: the risk of affecting the specific confidentiality and intimacy of the doctor-patient relationship that allow the individual, in a situation of vulnerability due to illness, to open up in person, which is very important both from a therapeutic and a human point of view.

Both the National Directions of 2020 and the Ministerial Decree on telemedicine requirements of September 2022 devote more attention to these aspects: for instance, it is provided that the televisit can never be the sole means for conducting the doctor-patient relationship, nor can it automatically be considered a substitute for the first in-person medical examination.

However, these provisions do not seem able to dispel all doubts. Is it possible to recreate the "safe place" of the physician-patient relationship in the virtual world, in the "non-place" of telemedicine,[54] in that "distance" that nevertheless remains in spite of (or because of) the use of technologies?

Another issue deals with the trend toward combining digital tools for telemedicine and artificial intelligence techniques.

Telemedicine and artificial intelligence represent a combination that has great potential for transforming treatment pathways and the organization of health services.[55] The use of algorithms to support medical decisions can certainly enable the identification of highly effective disease-management strategies and therapies and equips the physician with an uncommon predictive ability.

Nevertheless, the processing of algorithms, especially the more advanced ones, is not always intelligible and there can be grey areas in the operation: this is the issue of the so called "black box".[56] That is, there are cases in which programmers themselves are unable to understand the steps taken by the algorithm nor its future developments, a problem that concerns physicians all the more, as they are certainly not computer technicians. It was therefore pointed out that difficulties in understanding the reasons and processes of certain algorithms can undermine confidence in such tools even in those who interpret them, i.e. the physician, who is required to give complete information to patients, as well as in patients themselves, thus ultimately undermining the legitimacy of clinical decisions.[57]

5.1. *New and old inequalities generated or exacerbated by digital health. Further insights into the physician-patient relationship*

Telemedicine can certainly be said to be a tool of equality in that it can bring care and treatment to those who would otherwise be deprived of them due to the lack or scarcity of healthcare personnel or nearby facilities. Think of the case of those who live in remote locations or otherwise without health services.

However, the use of increasingly advanced technologies also brings problems from the point of view of accessibility to them. That is, at an individual level, the critical issue of the exclusion of those who do not have access to, or are unable to consciously use the technologies on which digital services depend. This is the so-called digital divide, which may be caused by multiple factors − geographical, economic, gender, cultural, religious, language and generational − often mutually influencing each other.

It can be observed that there is a tragic "circularity": the existence of disadvantaged situations underlies the digital divide, which in turn worsens existing inequalities.[58] Think of the elderly and the poor (often, moreover, the two situations coincide) or of young people living in disadvantaged contexts: age, frailty, lack of resources might make it impossible or difficult to access online

[54] "How to recreate in the non-place mediated by technological tools, however clever, that safe space necessary for a vulnerable subject to expose himself to medical evaluation?": this is the question posed by F.E. Brozzetti, G.M. Cannella and A. Randazzo, *Telemedicina, teleassistenza e intelligenza artificiale in un sistema socio-sanitario di prossimità: nuovi paradigmi etico-giuridici,* cit., 278.

[55] For an analysis of such potentials see A.E. Tozzi, *Il connubio tra telemedicina e intelligenza artificiale per un salto di qualità nelle cure*, in *Monitor*, 2021, 46, 39 *et seq*.

[56] The reference is to the book by F. Pasquale, *The Black Box Society*, Cambridge, MA, Harvard University Press, 2016.

[57] In this regard see M. Fasan*, La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del Coronavirus*, in *BioLaw Journal – Rivista di BioDiritto*, 2020, 1, 682-683.

[58] Hints on this aspect can be read in E.Mª Menéndez Sebastián and Javier Ballina Díaz, *Digital Citizenship: Fighting the Digital Divide*, in *Erdal*, 2/2021, Issue 1, 155.

services, which reverberates negatively on the condition of the person, aggravating his or her difficulties.

The NRRP has funding lines aimed at overcoming the digital divide,[59] but one cannot help but wonder whether this is enough to address the complexities that arise from accessing and using digital health.

The guidelines of the Ministerial decree of September 2022 show a more mature awareness of these issues than in the past and take into more consideration the "eligibility"/"enrollment" of the patient "from the clinical, technological, cultural point of view and autonomy or availability of a caregiver, if necessary, in the use of telemedicine services" and the "digital literacy of the patient and/or caregiver".

Clinical eligibility is at the sole discretion of the physician. Regarding the other profiles, there are quite a few uncertainties about the parameters for evaluating such conditions and situations and the subjects in charge of this assessment.

Finally, one should not overlook the case of those who do not adhere to the prevailing digital society model of information, which in its totalizing dimension affects everyone's freedom. Here, too, there are consequences in terms of exclusion and discrimination.[60]

As to this aspect, the doctor-patient relationship, within which one can assess who is suitable for telemedicine services and who is not, comes again into consideration. Cultural eligibility does not only mean the ability to know how to use certain ICT tools; the concept can also encompass cultural attitudes toward them.

Based on the above considerations, the silence in the September 2022 Decree on the patient's informed consent for activation of telemedicine services, which was instead provided for in both the 2014 and 2020 Guidelines and Directions,[61] is incomprehensible.[62]

5.2. *Telemedicine and the essential levels of care (the so called "Lea sanitari")*

Digital health also deeply affects the supply of healthcare services, as shown by the depicted evolution of telemedicine. In assessing its impact on the latter a first issue concerns its relationship with the "essential levels of care", in Italian the so-called "Lea sanitari", which are the services and benefits that the National Health Service is required to provide to all citizens, free of charge or upon payment of a participation fee (ticket).[63]

The "Lea sanitari" or, simply, "Lea" are the concretization in healthcare of the Constitutional provision relating to the "determination of the essential levels of services and benefits concerning civil and social rights that must be guaranteed throughout the national territory". By virtue of this competence, provided by second paragraph, letter m), of article 117 of the new Title V of the Italian Constitution, the State legislature has a fundamental tool to ensure throughout the Country an adequate uniformity of treatment in terms of the rights of all subjects, including the right to health.[64]

[59] See investment 1.7, also with reference to the population groups most exposed to this issue.

[60] The issue has been studied, for example, with reference to those who do not adhere to the technological model that underlies the smart-cities phenomenon: see F. Fracchia and P. Pantalone, *Smart City: condividere per innovare (e con il rischio di escludere?)* (25 novembre 2015), in *Federalismi.it*, 22, 2015, in partic. 23 *et seq*. More generally, on the discriminations that originate in contemporary algorithmic societies may we refer to V. Molaschi, *Algoritmi e discriminazione*, in M. Andreis, G. Crepaldi, S. Foà, R. Morzenti Pellegrini and M. Ricciardo Calderaro (eds.), *Studi in onore di C.E. Gallo*, Turin, 2023, vol. I, 355, and in *Fundamental rights*, https://fundamentalrights.it, 2022, 2, 19.

[61] On this point the 2020 National Directions stipulate that, in order to access the telemedicine healthcare service, the patient must give express informed consent to telemedicine healthcare treatment after being made aware by the physician about the following: the precise manner in which the service is to be performed, the objective of the service, the typical benefits and risks of providing telemedicine services, as well as how his or her personal data are managed, how to contact the data controller or processor, and what his or her rights are as a data subject.

[62] See C. Anderlini, *Approvate le linee guida per i servizi di telemedicina, il decreto del ministero della salute* (November 24, 2022), in studiolegalestefanelli.it/approfondimenti/linee-guida-telemedicina, who considers this lack of provision a "major absence", which, in any case, does not rule out the possibility that this tool could still be implemented by regions and autonomous provinces.

[63] The literature on the essential levels of care is very extensive: for a general overview see C. Tubertini, *Pubblica amministrazione e garanzia dei livelli essenziali delle prestazioni. Il caso della tutela della salute*, Bologna, Bononia University Press, 2008. Moreover, may we refer to V. Molaschi, *I rapporti di prestazione nei servizi sociali. Livelli essenziali delle prestazioni e situazioni giuridiche soggettive*, Turin, Giappichelli, 2008.

[64] On the guarantee of the right to health in Italy see, *ex multis*, R. Balduzzi and D. Servetti, *La garanzia costituzionale del diritto alla salute e la sua attuazione*

Indeed, scholars have referred to the essential levels as "the new name for equality".[65]

Are telemedicine services part of the "Lea"? Do they belong to this crucial pillar of the health offer of the Italian NHS?

Answering this question is not easy and requires going back over some of the stages of the gradual introduction of telemedicine in the healthcare system.

In this regard, it should be recalled that article 3 of the State-Regions Agreement establishing the Guidelines on telemedicine of 2014 provided that the regions' transposition of the Guidelines would be assessed during the annual verification of regional health performance by the Permanent Committee for the Verification of the Essential Levels of Care (Comitato permanente per la verifica dell'erogazione dei Livelli Essenziali di Assistenza), called, for short, Lea Committee (Comitato Lea).[66] As of 2018, all regions have adopted the Guidelines through their own resolutions.

However, the inclusion of telemedicine in the "Lea" cannot be derived from this provision. As known, guidelines are an example of *soft law*.[67] This type of acts, which encompasses, together with guidelines, codes of conduct, good practices, standards and so on, is aimed at harmonizing actions and behaviors in certain sectors, especially those characterized by a high rate of innovation and technical-scientific complexity, but, unlike laws and other regulatory sources, are not legally binding. Therefore, the aforementioned provision of the State-Regions Agreement was a way to give some kind of binding force to a *soft law* act.[68]

Nor does the fact that subsequent National Directions of 2020 stated that the national/regional regulatory framework governing access to the various essential levels of care applies to all healthcare services delivered remotely determines this inclusion. Indeed, they aim to define a framework for the supply of telemedicine services particularly as to their economic quantification. They do not grant a right to have telemedicine services.

The idea of digital "Lea" is perhaps *in nuce* in the Ministerial Decree of September 21, 2022, defining, as already said, the guidelines regarding telemedicine functional requirements and service levels, where the concept of "minimum services" appears. The Decree states that the minimum services to be provided by the regional telemedicine infrastructure are as follows: televisit, teleconsultation,[69] telemonitoring and telecare.

However, it cannot be said that this Decree embodies the "Lea".

The Italian Constitutional Court, in particular in decisions 88/2003 and 134/2006, has clearly defined the process for determining them. Given their strong impact on the exercise of functions in matters assigned to the legislative and administrative powers of regions and autonomous provinces, the Court has ruled that the choices concerning them are made, at least in general outlines, by State law, which must determine appropriate procedures and precise formal acts for further specification and articulation.

nel Servizio sanitario nazionale, in R. Balduzzi and G. Carpani (eds.), *Manuale di diritto sanitario*, Bologna, il Mulino, 2013, 13 *et seq*.; R. Ferrara, *Il diritto alla salute: i principi costituzionali*, in *Trattato di biodiritto*, directed by S. Rodotà, P. Zatti, vol. V, R. Ferrara (ed.), *Salute e sanità*, Milan, Giuffrè, 2010, 3 *et seq*.; Id., *L'ordinamento della Sanità*, Turin, Giappichelli, 2020, 39 *et seq*.; Id., *Salute (diritto alla)*, in *Digesto delle Discipline Pubblicistiche*, vol. XIII, Turin, Utet giuridica, 1997, 513 *et seq*.; D. Morana, *La salute nella Costituzione italiana. Profili sistematici*, Milan, Giuffrè, 2002; B. Pezzini, *Principi costituzionali e politica nella Sanità: il contributo della giurisprudenza costituzionale alla definizione del diritto sociale alla salute*, in C.E. Gallo and B. Pezzini (eds.), *Profili attuali del diritto alla salute*, Milan, Giuffrè, 1998, 1 *et seq*.; M. Luciani, voce *Salute* (diritto alla salute – dir. cost.), in *Enc. giur.*, Roma, Treccani, 1991, vol. XXVII; Id., *Il diritto costituzionale alla salute*, in *Diritto e Società*, 1980, 769 et seq.; B. Caravita, *La disciplina costituzionale della salute*, in *Diritto e Società*, 1984, 21 *et seq*.

[65] In these terms E. Balboni, *Livelli essenziali: il nuovo nome dell'eguaglianza? Evoluzione dei diritti sociali, sussidiarietà e società del benessere*, in E. Balboni, B. Baroni, A. Mattioni and G. Pastori (eds.), *Il sistema integrato dei servizi sociali. Commento alla legge n. 328 del 2000 e ai provvedimenti attuativi dopo la riforma del Titolo V della Costituzione*, Milan, Giuffrè, 2003, 27 et seq.

[66] The State-Regions Agreement of 23 March 2005 established at the Ministry of Health the Lea Committee (Comitato Lea), which is entrusted with the task of verifying the provision of the essential levels of care under conditions of appropriateness and efficiency in the use of resources, as well as the congruity between the services to be supplied and the resources made available by the National Health Service.

[67] On the use of *soft law* as a regulatory method in the field of e-Health see M. Campagna, *Public and private participation in digitalised healthcare*, in this issue of *Erdal*.

[68] See M. Campagna, *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19*, 610; C. Botrugno, *La diffusione dei modelli di cura a distanza: verso un "diritto alla telesalute"?*, 173.

[69] Teleconsultation concerns the relationship between professionals.

Moreover, the procedure must respect the principle of loyal cooperation, deemed a "constitutionally necessary principle".[70] The provision of health services is not unilaterally imposed by the State, but must be agreed upon in certain aspects with the regions, which are responsible for the planning and organization of health services in the territory, up to their actual supply through their regional healthcare systems.[71]

The procedure for identifying the essential levels of healthcare has most recently been regulated by article 1, par. 553 *et seq*., Law 208/2015: according to it, they are defined and updated by Decree of the President of the Council of Ministers on the basis of an Agreement achieved in the State-Regions Conference. At present, the "Lea" have been determined by the Decree of the President of the Council of Ministers of January 12, 2017.

The aforementioned Ministerial decree of September 2022 regarding telemedicine is merely a ministerial-level transposition of guidelines, without any underlying State-Regions Agreement, a procedural aspect that, as seen, is very significant.[72] On the basis of these arguments, it cannot yet be said that telemedicine is the object of a right, granted through the "Lea".

From this point of view, it may also be interesting to note the fact that, according to the same Decree of September 2022, no new or additional burdens on public finance arise from its implementation (art. 2). The planned activities are carried out with the human, instrumental, and financial resources available under current legislation, and there is no special economic appropriation designed to guarantee the provision of telemedicine services.

5.3 *Telemedicine and healthcare organization. Implications for the principle of equality*

Further observations concern the huge organizational effort required by the implementation of digital health. It is sufficient to think of the slowdowns that have marked the history of telemedicine, as well as other digital tools, like the electronic health record.

The organizational commitment is exceedingly complex as it involves integrating innovative modes of care with traditional ones.[73]

Organizational issues are all the more relevant insofar as the level of guarantee of the right to health is not only a matter of services provided. The effectiveness of the right is affected by organizational choices: as some scholars have pointed out, the fulfillment of subjective legal situations – rights or interests – "appears historically and politically subordinate to the organizational moment".[74]

Quite often, inequalities in health protection depend on organizational choices and dynamics. Emblematic in this regard are the disparities between the different Italian regional health systems and, in particular, the differences between Northern and Southern healthcare.

Will the recently approved guidelines on telemedicine be enough to ensure homogeneity in the delivery of remote services?

For sure, they represent an important step in supporting from a technical and functioning

[70] For this statement see Constitutional Court decision n. 98/2007.

[71] For the application of these principles see Constitutional Court decision no. 114/2022.

[72] Similar comments were made with reference to the "Guidelines for the Implementation of the Electronic Health Record" ("Linee guida per l'attuazione del Fascicolo sanitario elettronico") adopted by Decree of the Ministry of Health of 20 May 2022: see N. Maccabiani, *Tra coordinamento informativo e livelli essenziali delle prestazioni: il caso del Fascicolo Sanitario Elettronico*, in *federalismi.it*, 2023, 12, 250. In the present case, moreover, the decree was issued after hearing the Permanent Conference for Relations between the State, Regions and Autonomous Provinces of Trento and Bolzano and not on the basis of an agreement with it. The subject of criticism, therefore, was the degree of collaboration between State and territorial autonomies, which was not in accordance with the Constitutional jurisprudence and the legislative approach to the essential levels.

[73] M. Campagna, *Linee guida per la Telemedicina: considerazioni alla luce dell'emergenza Covid-19*, cit., 610; C. Botrugno, *La diffusione dei modelli di cura a distanza: verso un "diritto alla telesalute"?,* 609.

[74] In these terms see G. Corso, *I diritti sociali nella Costituzione italiana*, in *Rivista trimestrale di diritto pubblico*, 1981, 3, 762. On the impact of organization on the right to health and, more in general, on the right to social services, one may refer to V. Molaschi, *La rilevanza dell'organizzazione dei servizi pubblici sull'effettività dei diritti sociali*, in M. Renna, C. Micciché and P. Pantalone (eds.), *La partecipazione dei cittadini all'organizzazione dei servizi sociali. Il caso della metropoli milanese*, Napoli, Editoriale Scientifica, 2020, 27 *et seq*.; Id., *Programmazione e organizzazione dell'equità in sanità. L'organizzazione come "veicolo" di eguaglianza*, in *BioLaw Journal – Rivista di BioDiritto*, 2019, 2, 51.

point of view regions and autonomous provinces for the definition and implementation of project initiatives on telemedicine services within a common framework. From this perspective, it is significant that they have been acknowledged in a decree, which is not a *soft law* act, as the previous guidelines were: this means that precisely with a view to ensuring greater uniformity it has been decided to give more stringent guidance with greater constraint.

However, the problems concerning the uneven distribution of infrastructure and resources between the various Italian regions still remain, with consequences in terms of digital divide. This could heighten once again the already-existing inequalities that characterize the different national territorial areas, with repercussions on the guarantee of the right to healthcare.[75]

Moreover, the NRRP intervention in the field of telemedicine mostly consists of funding telemedicine projects proposed by regions: the Plan deservedly rewards the regional "spirit of initiative". However, this policy could reveal some points of "weakness": the risk that the already-more-virtuous and technologically-advanced regions could take advantage of the measure and that the others, more in difficulty, could once again fall behind.[76]

In this regard, it should be noted that, according to the Report on the status of implementation of the National Recovery and Resilience Plan of May 31, 2023, the goals inherent in telemedicine have been subsequently specified by providing for at least one project per region by 2023 (considering both the projects that will be implemented in the single region and those that may be developed within consortia between regions).

A push, however, in the direction of greater "digital uniformity" in healthcare will come from the National Telemedicine Platform. The latter, in fact, promoting the adoption of telemedicine organizational and process best practices, is aimed at bridging the gap between territorial disparities. In addition, it will achieve greater integration between regional health services and better interoperability with central systems deployed nationwide, thereby improving the accessibility and quality of healthcare delivery.

[75] On these issues see, more in general, A. Morelli, *Il diritto alla salute nell'era digitale: profili costituzionalistici* (18 December, 2012), in *mediaLAWS*, http://medialaes.eu, paragraph 4.

[76] According to L. Ferraro, *La telemedicina quale nuova (e problematica) frontiera del diritto alla salute*, 850-51, it is interesting to note that, based on the mapping of experiences done by the Ministry of Health (dated 2018 and updated in 2021), although the best data on activated telemedicine experiences concern the North of Italy, there is not an excessive gap compared to the South. The data, both positive and negative, varied across different areas of the Country. The Ministry of Health document can be found at the following link: www.salute.gov.it/imgs/C_17_pagineAree_2515_2_file.pdf.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 169-176
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 12

*The Development of Telemedicine and its Application Possibilities in Hungary**

Gabriella Berki
(Assistant Professor Department of Labour and Social Law at University of Szeged)

Gergely Toth
(Assistant Research Fellow of the Department of Civil Law at University of Miskolc)

Zsolt Czékmann
(Associate Professor Head of Department of Administrative Law at University of Miskolc)

ABSTRACT The aim of this study is to present the emergence and spread of telemedicine in Hungary. How did we move from landline telephones to the use of ICT devices and applications, what legal developments were needed to make this possible. We will look at the major turning points in this story, in particular the impact of COVID and the entry into force of GDPR, because both led to paradigm shifts in different but significant ways. The focus of the study is on the development of the Hungarian legal environment and how it defines certain concepts of telemedicine.

1. *The development of the concept of telemedicine[1] in the international space*

For a long time, the concept of telemedicine did not correspond to any single, well-defined concept. This is clearly demonstrated by the fact that no fewer than 107 different definitions in the literature are included in a 2007 WHO study.[2] It is also clear from this that, in such situations, it is difficult for the legislator to promulgate a systematic codification where no consensus can be found even on the main rules.

With regard to international practices, the following four main sub-fields of telemedicine can be defined and delimited based on the functionality of the telemedicine devices: during the remote consultation, not only the patient's treating doctor(s), but also a remote doctor or other specialist staff are involved in the diagnosis through communication tools (e.g. the doctor and the pharmacist consult on the phone); remote manipulation occurs when a remotely-controlled examination or intervention is carried out; during telediagnosis, the person performing the examination that forms the basis of the diagnosis and the person making the diagnosis (e.g. the person who prepares the findings) are spatially separated, but they are in an interactive relationship; in the case of remote monitoring or telemonitoring, the data about the patient for the medical personnel are replaced by signal receivers and signal transmitters.[3]

An example of the earliest practical application of telemedicine can be seen in the

* Article submitted to double-blind peer review.

[1] Although the creation of the term telemedicine can be linked to the name of the American Thomas Bird in the 1970s, its roots actually go back much longer, and the theoretical foundations of its implementation were made possible by the rapid development of telecommunication networks and devices at the end of the 19th century and the beginning of the 20th century. In April 1924, Radio News Magazine was published with a cover called "The Radio Doctor-Maybe", in which the possibility of real-time, online image communication and its medical use appeared for the first time, and in 1925, it presented the "prediction" of telemedicine to the Science and Invention magazine, because this issue featured writer and inventor Hugo Gernsback's device called "Teledactyl", which seemed quite futuristic in the conditions of the time, and which, according to the ideas, would have worked in such a way that while the doctor was moving his robotic fingers in his office, they were moving on the patient in the same way. This device can also be seen as a prototype of telemedicine, which implements remote examination of the patient (http://eta.bibl.u-szeged.hu/2188/3/2_a_telemedicina_rvid_trtneti_ttekintse.html,12.12.2023).

[2] A WHO report (Telemedicine, Opportunities and developments in Member States Report on the second global survey on eHealth, in Global Observatory for eHealth series, 2010, vol. 2, www.who.int/goe/publications/goe_telemedicine_2010.pdf), cites S.P. Sood *et al*., *Differences in public and private sector adoption of telemedicine: Indian case study for sectoral adoption*, in *Studies in Health Technology and Informatics*, 2007, 130, évf. 257–268.

[3] Telemedicine practice (note). http://biofiz.semmelweis.hu/index.php?p=oktatas&mid=2&a=tantargy&id=252.

1920s in Norway, when the Haukeland hospital organized a medical service via radio for the crew of ships at sea. In the United States of America, the use of telemedicine was primarily brought about by the need to overcome long distances, and it was a significant solution for the medical care of relatively-isolated communities, islanders, and workers in polar and desert regions, as for example in the case of the Nebraska Psychiatric Institute, where since 1955 a closed-chain audio-visual link was established with the Norfolk State Hospital, approximately 200 km away, using a television system. The other direction of the initial development was the help provided to space research and military activities primarily through the activities of NASA, as a result of which by 1975 there were already 15 telemedicine programs in the United States, the best known of which was the STARPAHC program. Within the framework of this program, between 1972 and 1976, health care was provided to the residents of a remote Indian reservation in the state of Arizona and to the astronauts in outer space at the time, which was realized by placing medical equipment (including EKG and X-ray machines) in a truck, connected via microwave and sound transmission to a hospitals outside the district, provided with the necessary technical background by NASA. Also, with the help of NASA, using its ATS-1 satellite, it was possible to connect 26 villages in Alaska via 4 ground transmitting stations and receiving station located in the Native Medical Centre in Anchorage. With the involvement of the ATS-6 satellite, NASA provided assistance after the earthquake in Mexico City in September 1985, and in 1989, after the earthquake in Armenia, a connection for the transmission of voice and documents was provided between the medical centre in Yerevan and 4 American medical centres.[4]

2. *The emergence of telemedicine in Hungary*

As everywhere in the world and in Central Europe and especially in Hungary, in the 1990s the development of telemedicine was given new impetus by the spread and rapid development of computer networks and mobile phones. The advantages of using telemedicine for the health-care system and the patients appear both directly and indirectly, in a 2010 Hungarian study we can find the following:[5] a) one of the direct benefits is that specialist medical care becomes more accessible to those that were previously challegend by space and time constraints; the length of stay in health-care facilities is reduced; fairly long waiting lists can be shortened; it becomes possible to obtain secondary or even third-party expert opinions; the use of resources can be better optimized; health institutions providing teleconciliation can operate with fewer staff, but at the same time earn more income; material savings can also be expected, and patients and medical professionals can also save significantly on travel costs and time; b) it appears as an indirect benefit that, with the help of telemedicine, high-level health services can reach even remote and sparsely-populated areas; where such professions would otherwise not be available, thereby providing more effective, even life-saving consultations and fostering increasing self-sifficiency of the elderly population, since home monitoring of the condition of the elderly provides security and, if necessary, even enables immediate intervention.

A summary[6] published in 2013 presents the ethical, legal and financing issues arising in connection with the practical application of telemedicine in Hungary in a more differentiated way, as well as the emerging problems awaiting regulation, which point to the conditions that make it difficult for telemedicine to be effective in our country despite its obvious advantages.

The root of these problems mostly stems from lack of information and a high degree of distrust towards the new method (which does not even arise in North America or Scandinavia, for example), and on the other hand, the still-unresolved issues related to its application.

From an ethical point of view, the strengths of communicating via telemedicine are: avoiding long waiting times for the patient; leaving messages which allows even off-line

[4] G. Harsányi, *Telemedicine*.

[5] A. Ficzere, *Interdisciplinary Hungarian Healthcare,* in *Informatics And Management In Healthcare* 1588-6387 1789-9974 9, vol. 1, 2010, 48-50. www.imeonline.hu/article.php?article=2010._IX./1/telemedicina.

[6] L. Daragó, Z. Jung, F. Ispán, R. Bendes and E. Dinya, *Advantages and disadvantages of telemedicine*, Summary notice, 1167. https://repo.lib.semmelweis.hu/bitstream/handle/123456789/5178/2388209.pdf?sequence=1.

contact; providing patients' continuous monitoring; setting automatic alarms; and allowing for the possibility of statistical analysis of the data.

On the other hand, telemedicine also has weaknesses, namely: the doctor-patient relationship becomes rare, thereby narrowing the classic and traditional relationship between the all-knowing doctor and patient; and generally impersonality fosters distrust.

During the implementation of telemedicine, with medical participation, it is possible to use telemedicine community fora as well as teleconsilium, which can also provide access to family members.

From an ethical point of view, telemedicine may contain the danger that patients would accept misleading or downright harmful suggestions in the online space, on social media sites, or they start self-medicating without any professional supervision on the basis of information found on the Internet.

From an ethical point of view, unauthorized access to data can be an additional source of danger, which already raises data-protection and data-management concerns.

When examining the legal aspects of telemedicine, the summary statement highlights the decennial lack of professional regulation and court practice, as well as the lack of domestic case-studies and the fact that foreigners cannot adapt to the domestic legal environment. Despite the proposals formulated ten years ago, the legislator has not yet succeeded in implementing any systematic legal regulation regarding telemedicine, but some of its directions give reason for confidence.

3. *The Hungarian legal regulations*

In Hungary, Act CLIV of 1997 on Health Care (Eütv.) contains only a few provisions regarding telemedicine, including electronic records of infectious patients[7] and telemedicine services based on facial identification.[8] Surprisingly, neither this legislation, nor Act XLVII of 1997 on the management and protection of health and related data (Eüak.) do specifically describe the concept of telemedicine.

The definition is found in 28/2010. (V.12.) EüM decree,[9] according to which telemedicine is: "a healthcare service in which the person receiving the care and the person providing the care do not meet directly, the connection is established through some remote data transmission system".

The 9/2012. (II. 28.) NEFMI decree[10] contains the legal provisions that determine how health-care providers can account for the financing due to the health care services provided.

It should be emphasized that if the health-care provider offers health-care services via telemedicine, the settlement is not conditional on the patient's personal appearance before the health care provider.

Annex 6 of the decree contains the procedures and services that patients can use even without a personal presence, these are as follows:

- Control examination, consultation outside the clinic or within the framework of telemedicine (OENO code:[11] 11302)
- with EEG telemetry (OENO code: 12074)
- with ECG telemetry (OENO code: 12604)
- Application of transtelephonic ECG in acute cardiac pathologies (OENO code: 12607)
- Application of transtelephonic ECG in postoperative cardiac pathologies (OENO code: 12608)
- Transtelephonic ECG in elective cases (OENO code: 12609)
- Use of transtelephonic ECG in acute cardiac pathologies during rescue tasks (OENO code: 12611)
- Preparation and sending of a sample sent by telepathology during colonoscopy (OENO code: 29004)
- Evaluation of the sample sent by telepathology during colon screening (OENO code: 29005)
- Additional score in case of issuing a second expert opinion in the context of

[7] Eütv. (1) of § 61.
[8] Eütv. 106/A. § - 106/C. §.

[9] 8/2010. (V. 12.) EüM decree on the system of professional criteria and professional policy priorities to be applied during the procedure related to the inclusion of health technologies used in curative-preventive procedures into health insurance financing, as well as the administrative service fees to be paid for certain procedures related to their inclusion.
[10] 9/2012. (II. 28.) NEFMI decree on the definition of outpatient specialist care activities that can be financed at the expense of the Health Insurance Fund, the accountability conditions and rules applicable during use, and the accounting of performances.
[11] International Classification of Medical Procedures.

colon screening (OENO code: 29006)
- Teleradiographia dentalis (OENO code: 31060)
- Pain monitoring and computer evaluation/case (OENO code: 89614)
- Documented psychiatric consultation by phone (OENO code: 96003)

Therefore, based on the decree, the accounting rules for all these procedures and interventions that can be reported in the "T" care category, i.e. health services provided via telemedicine, if they are not defined separately, are the same as the accounting rules for the care and interventions reported in care based on personal presence.

60/2003. ESzCsM decree,[12] among other things, fixes the parts and minimum conditions of teleradiology and teleconsultation. According to the decree, "teleradiology is a type of telemedicine activity, when the recordings of imaging diagnostic examinations are transmitted electronically from one location to another for the purpose of examination or consultation".

The part of teleradiology is
- telediagnostics (remote diagnostics): meaning an image evaluation carried out after the end of the examination, far from the place of imaging, which can be a first or second finding. In the case of tests where an evaluation by two doctors is required, it may trigger an evaluation by one or both doctors.
- teleconsultation: image evaluation at the same time as imaging or shortly after, the result of which affects the course of the examination, or re-evaluation of a previous, already-evaluated examination according to new aspects."[13]

Based on the telemedicine provisions of the decree, healthcare providers must comply with several regulations in order to be able to provide healthcare services within the framework of telemedicine.

It is the duty of healthcare providers to provide the appropriate info-communication device, the medical equipment required for the given care, the procedure for telemedicine care and the patient information sheet.[14]

Pursuant to the decree, general practitioner and pediatric surgeries must have a telephone, mobile phone or computer with a broadband internet connection suitable for remote consultation. In the latter case, in addition to stable data transmission, an additional condition is data security, for which the use of the appropriate security protocol is mandatory, VPN and https protocols are recommended.

If legislation requires the use of a video connection for the performance of a specific medical procedure, then the devices for creating a video connection must also be considered info-communication devices. The healthcare provider must also ensure clear identification of the patient.[15]

The decree not only establishes minimum objective conditions, but also the competences of the specialist doctor, healthcare worker and clinical psychologist, who must possess a higher level of specialist qualification in their given field of expertise.

In accordance with the provisions of the Act on the Management and Protection of Health and Related Personal Data, one can perform the following activities within the framework of telemedicine:
- make a diagnosis and therapeutic proposal
- provide advice and consultation
- provide patient management
- give a referral
- provide care
- perform therapy and rehabilitation activities
- prescribe medicine
- prescribe medical aids that can be ordered via electronic prescription.[16]

Among the provisions in force regarding telemedicine, EÜak should be mentioned. 35/M.§ and 39/2016. (XII. 21.) EMMI Decree 20/A. § and 20/B. §, which describe access by the user and transmission between users of the recording or other digital-image information made by the imaging-diagnostic procedure of the affected person through the Electronic Health Service Area (EESZT), as well as the rules of the electronic consultation conducted in the system of the EESZT.

In order to transmit digital images, the operator of the EESZT keeps a register, which requires the TAJ number or other identifier of the person concerned. From the point of view of data management, it should be mentioned

[12] 60/2003. (X. 20.) ESzCsM decree on the professional minimum conditions necessary for the provision of health services.
[13] Annex 2 to 60/2003. (X. 20.) ESzCsM decree: The minimum conditions necessary to carry out the activities.
[14] Section 3 (1) point g) of ESzCsM decree.
[15] ESzCsM decree 3.§ 2) point b).
[16] Section 9(7) points a)-h) of ESzCsM decree.

that the data concerning the data subject in the register are deleted by the operator ten years after the death of the data subject.[17]

In the case of an electronic-remote consultation, we can distinguish between a doctor who initiates a consultation (that is, requests a consultation) and one who gives a consultation (who accepts the request).

Only the doctor who has registered separately for the service is entitled to initiate the electronic consultation and accept the request.

In relation to the electronic consultation, both aforementioned decrees stipulate that operators ensure their conduct through the EESZT in the event that the doctor invited to the consultation ensures the conduct of the electronic consultation, the consultation accepts the request and is entitled to know the data concerning the person concerned.[18]

When initiating an electronic remote consultation, the attending physician requesting the consultation compiles a list of all medical documents (including recordings of imaging diagnostic procedures) that someone wishes to share with the attending physician during the remote consultation. If the treating doctor who gave the consultation accepts the request, the EESZT will grant access to the documents on the list if it does not conflict with the declaration made in the self-determination register of the concerned person. The treating physician giving the consultation transmits his/her medical opinion given in the framework of the electronic remote consultation to the treating physician requesting the consultation via the EESZT system.[19]

Although telemedicine was already part of Hungarian healthcare before 2020, the upswing in its practical application is still due to the COVID-19 period, because the pandemic urged the legislator to provide solutions for the healthcare personnel as soon as possible.

The 157/2020 (IV.29.) Government decree[20] entered into force during the state of emergency of the epidemic period. According to it and to 9. § (7) of 60/2003 (X.20) ESzCsM decree on the professional minimum conditions necessary for the provision of health services, patients' physical presence is not a condition for the provision of health-care services and financial accounting.[21]

Pursuant to the decree, telemedicine is considered to be an activity the purpose of which, in the patient's absence, the following services are provided:

- professional assessment of the patient's state of health,
- detection of diseases and their risks,
- definition of the specific disease(s),
- ordering additional tests necessary for a more accurate assessment of the patient's condition, starting medical treatment,
- determination of the effectiveness of the treatments listed above (remote consultation), and
- monitoring the patient's condition and establishing a diagnosis based on information available through remote-monitoring devices and other information-communication technologies.

At the same time, in the decree, the legislator not only regulated the concept, principles and purpose of telemedicine, but also the health services that can be provided within the framework of telemedicine, in particular:

- patient management in the form of teleconsultation, which forms the basis of specialist teleconsultation,
- receiving statements regarding the patient's information, consent, and handling of their data
- pre-screening in the form of remote consultation, the purpose of which is to assess the need for care based on a personal meeting and the severity of the health condition,
- preliminary contact and data collection, which makes the care based on a personal meeting following the teleconsultation faster and more efficient,
- diagnosis and therapeutic proposal in the framework of remote consultation, as well as remote monitoring and remote diagnostic tools,
- order medication,
- control and follow-up care following previous care based on a personal meeting,
- organization of teleconference,

[17] Eüak. 35/M. § (1).
[18] Eüak. 35/M. § (2).
[19] EMMI decree 20/B. § (2).
[20] 157/2020. (IV.29.) Government Decree on certain health measures ordered during the state of emergency, (hereinafter: Government Decree) repealed. Based on Article 53 (4) of the Basic Law of Hungary. Invalid: as of the end of the state of emergency, June 2020. from 18.
[21] Government Decree § 1.

- issuing a referral,
- psychotherapy, crisis intervention, parent consultation, counselling, supportive psychotherapy,
- physiotherapy with teleconsultation tool,
- breastfeeding counselling
- nursing care and
- telephone, online or other forms of advice and consultation.[22]

The decree stipulates that the health-care provider certifies the above-mentioned services in the manner specified in the legislation on the management of health documentation, and develops its institutional protocol for the provision of these services.

The health-care provider must also ensure that an event-catalogue entry documenting the fact and participants of the examination is created in its own IT system, and thus in the Electronic Health Service Area, as well as a document certifying the examination from a professional point of view.[23]

Art. 7. § of the Government Decree lays down an additional obligation for health-care providers, as they must offer services that do not require the patient's personal presence and make them available via their website.

4. *Development possibilities of telemedicine and challenges related to data management*

In addition to telemedicine, concepts such as e-Health, telehealth, mhealth, which have different meanings, have appeared in recent decades. E-Health includes all services related to IT, telecommunications and health, an example of which is the Electronic Health Services Square (EESZT) operating in Hungary. Within the concept of ehealth, we can distinguish four major categories: ehealth devices, ehealth applications (applications), online pharmacies, and online medical advice.

EHealth devices are biosensors that collect information about users' health parameters, such as blood pressure and body weight.

Ehealth applications refer to different applications, including smart watches that measure physical activity, as well as the use of applications that support weight loss or even those related to contraception and fertility.

Online pharmacy means the purchase of medicines that are available without a medical prescription, sales are carried out exclusively electronically, online.

Online teleconsultations represent the largest part of the telemedicine segment, which means counselling between patients and doctors created exclusively through online channels.[24]

Telehealth is a broader concept than telemedicine, which also means information networks and health services that ensure public's health awareness. It includes telecare, which is primarily provided to the elderly or disabled, but also includes health information and professional education.[25]

The concept of mhealth (mobile health) includes all health solutions that are implemented with a mobile device, which can be not only a smartphone, but also any other wireless technology, for example mobile monitor systems or even wearable sensors.[26]

Regardless of the specific form of telemedicine, it can generally be said that it involves the handling of sensitive personal data, the legality of which is legal if and only if at least one of the following is met, based on Article 6 of the General Data Protection Regulation[27] (GDPR):

a) consent is given to the processing of personal data for one or more specific purposes
b) data processing is necessary for the performance of a contract in which the data subject is one of the parties, or it is necessary for taking steps at the request of the data subject prior to the conclusion of the contract;
c) data management is necessary to fulfil the legal obligation of the data controller;
d) data processing is necessary to protect the vital interests of the data subject or another natural person;
e) data processing is in the public interest or is necessary for the execution of a task performed in the context of the exercise of public authority delegated to the data controller;
f) data management is necessary to enforce the legitimate interests of the data

[22] Government Decree § 2 (2) points a)-n).
[23] Government Decree § 4 (1)-(2).
[24] R. Árpád, *Business and social trends and vision of eHealth*, www.ludovika.hu/blogok/itkiblog/2023/02/03/az-ehealth-uzleti-tarsadalmi-trendjei-es-jovokepe/.
[25] G. Berki, *What does telemedicine grow on? - the concept and development of telemedicine*, in *Acta Universitatis Szegediensis: forum: acta juridica et politica*, 2021, vol. 11, 3, 39-46.
[26] http://eta.bibl.u-szeged.hu/2188/3/1_bevezets.html.
[27] Regulation 2016/679 of the European Parliament and of the Council.

controller or a third party, unless the interests or fundamental rights and freedoms of the data subject take precedence over these interests, which require the protection of personal data, especially if the data subject is a minor.

In practice, private healthcare providers refer to several legal bases during their data management.

On the one hand, patients can also manage their data based on their voluntary consent, which is considered to be given by their behavior (i.e. simply by providing the data) during the voluntary use of health services.[28]

On the other hand, legislation may also require the processing of data as a requirement, cases of which may include the following in particular: official notification of work accidents, occupational diseases, infectious diseases or suspicions thereof, official communication of the results of certain screening tests, data management required for certain suitability tests, reporting of acute poisonings, fulfilment of official inquiries; interest in the treatment of a fetus or minor. In the case of certain, typically sexually-transmitted diseases, the names of the contact persons can be requested, and in the case of tuberculosis (TBC), health care-providers must forward data to the competent lung-care service.[29]

Data management is mandatory in the event that the patient is not fully capable of acting, in which cases the patient cannot refuse health care, as well as the associated data management.[30]

Data management is also mandatory if the patient is in immediate danger,[31] if his/her condition or lack of care endangers others,[32] or if he/she needs emergency or mandatory psychiatric treatment.[33]

In exceptional cases, data management may be based on the legitimate interests of other health-care providers or other persons, in which case data management is allowed upon consideration of several interests.[34]

The legal basis for data management can also be a contract between the healthcare provider and the patient (e.g. care and treatment contract).[35]

The basis of data management can also be cases where its realization is necessary due to the protection of the vital interests of the person affected by the data management or of another person, but the person in question is unable to consent to it due to physical or legal incapacity.[36]

In contrast to the above (that is, with regard to the legal grounds cited by private healthcare providers), domestic case law[37] takes the position that consent is not the legal basis for data processing related to the use of healthcare services, but can only be the legal basis for data processing in the case of subscriptions to electronic newsletters.

There can be no doubt that telemedicine is the future of the field of medicine. However, the legislator also has a serious task in order to clarify the detailed rules.

5. *Conclusion and a look to the future*

In conclusion, telemedicine in Hungary has come a long way from the 1990s to the present. The development has not been uninterrupted, the initial mistrust on the part of the parties (both health actors and patients) has been slowly dissolved, but finally the constraints, especially the restrictions introduced during the COVID epidemic, have broken through this wall. Unfortunately, the growing shortage of doctors in Europe is also pushing the healthcare system in Hungary towards telemedicine, especially in the case of primary care GPs. We do not want to give the impression that only coercion has led to the spread of telemedicine, and the last thing we want is for it to be a kind of forced solution.

We believe that it is possible to provide effective health care in the right conditions and in the right framework. If we take into account the development of technology,

[28] Regulation 2016/679 of the European Parliament and of the Council Article 6 (1) a), Article 9 (2) a), h); XLVII of 1997 Act § 12.
[29] Regulation 2016/679 of the European Parliament and of the Council (1) c), d), Article 9 (2) b), g), h), i); Act XLVII of 1997 § 13, 15/A.; 18/1998. (VI. 3.) NM Decree § 21.
[30] Regulation 2016/679 of the European Parliament and of the Council (1) c), d), Article 9 (2) c), h); Act CLIV of 1997 Section 20 (1).
[31] Act CLIV of 1997 17.§ (2) b).
[32] Act CLIV of 1997 17.§ (2) a).
[33] Act CLIV of 1997 199-200. §§; Regulation 2016/679 of the European Parliament and of the Council (1) c), d), Article 9 (2) c), g), h).
[34] Regulation 2016/679 of the European Parliament and of the Council Article 6 (1) f).
[35] Regulation 2016/679 of the European Parliament and of the Council Article 6 (1) b), Article 9 (2) f).
[36] Regulation 2016/679 of the European Parliament and of the Council Article 6 (1) d), Article 9 (2) c).
[37] BDT2021. 4391 Szegedi Ítélőtábla Gf.30.241/2020/12.

remarkable new paths are emerging. In Hungary, in the Electronic Health Services Area (EESZT) system, almost the entire patient journey and patient history is now available electronically (and all new events must be recorded, whether in public or private health services), providing doctors with a rare database available on a global scale. Combining this database with the latest technologies, in particular the data processing and prognostic capabilities of artificial intelligence, and the continuous monitoring capabilities of ICT tools (see mHealth), opens the way to the development of an alert system that can even automatically contact the doctor when necessary, based on the current state of the patient. Research into the development and application of this system is currently underway in several Hungarian research centres. The technology and the legislative environment are given, and in the case of data protection issues, there are still open questions due to the use of artificial intelligence, but the legislator will be forced to respond to this within the foreseeable future, so this direction of development seems promising for the future.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 177-185
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 13

*Primary Use of Data in the European Health Data Space Proposal: Its Impact on National Electronic Health Records from a Spanish Perspective**

Andrea Salud Casanova Asencio
(PhD. Assistant Professor of Civil Law at University of Murcia)

María Belén Andreu Martínez
(Full Professor of Civil Law at University of Murcia)

ABSTRACT ***The European Health Data Space represents an important advance in the context of the European Data Strategy, among other issues, in relation to the promotion of the rights of natural persons regarding the primary use of their health data, a matter in which it offers some novel solutions. The Proposal for a Regulation published in 2022, and currently in the process of being discussed, provides for a series of rights that, in practice, require a new configuration in the national medical records system of Member States such as Spain, which serves as a reference in this study.***

1. *Introduction*

The European Health Data Space (EHDS) constitutes the first data space proposal within the framework of the European Data Strategy.[1] The basic purpose of the EHDS is to create a health data exchange mechanism within the EU, establishing a series of rules, standards, common practices, infrastructure and a governance framework for the primary and secondary use of electronic health data. The regulation contained on primary use[2] is the one likely to have the greatest impact on the configuration of national medical records. In relation to primary use, the basic objectives of the EHDS and the Proposal for a Regulation of the EHDS (which will subsequently be referred to as "the Proposal") are to:

1) Strengthen natural person's control over their health data.
2) Establish standards specifications for Electronic Health Records (EHR) systems.
3) Create a mandatory cross-border infrastructure for primary use of data.

The impact of these measures at the European level is clear, with the creation of instruments that must be available at a supranational level, as is the case with mandatory cross-border infrastructure for primary use. However, many of the provisions envisaged have a no less important effect on the internal legal systems of the Member States; and, in particular, the measures established to promote the rights of natural persons in relation to their health data have the potential to require important reforms in this regard. We will focus on these issues in the following pages, taking as a reference, in particular, the Spanish system.

2. *Configuration of medical records in the Spanish health system*

In the Spanish case, the medical record system is complex, since competence in health matters is shared between the State and the autonomous regions known in Spain as Autonomous Communities (CCAA), and the management of public health care corresponds to the health services of the CCAA. This has

* Article submitted to double-blind peer review.

[1] See European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European strategy for data", COM(2020) 66 final, 2020. Accessible here: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0066.
See also, in general, D. Horgan, M. Hajduch, M. Vrana, J. Soderberg, N. Hughes, M.I. Omar, J. A. Lal, M. Kozaric, F. Cascini, V. Thaler *et al*, *European Health Data Space – An opportunity now to grasp the future of data-driven healthcare*, in *Healthcare*, no. 10, 2022, 1629, accessible here: https://www.mdpi.com/2227-9032/10/9/1629.

[2] Which is defined in the Proposal as "the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services" (Art. 2.2.d).

given rise to the existence of eighteen health systems in Spain, each with its own model and medical record infrastructure.

The regional systems are, as of today, highly digitalized, although the regulation to develop said digitalization is scarce.[3] The high degree of digitalization offers great functionalities in the use of medical records, especially to professionals, but also to patients (through the different patient care web portals of the different health systems). However, access to these digitized medical records from the CCAA is in principle designed for the scope of the CCAA itself, so if the patient travels to other places in Spain, said information is not accessible neither to the patient nor to the health professionals.

In view of the above, the Digital Medical Record of the National Health System, known in Spanish as "Historia Clínica Digital del Sistema Nacional de Salud" (HCDSNS) was promoted, at a national level, by the Spanish Ministry of Health (in collaboration with the Autonomous Communities). Its purpose was to make available to citizens their existing health data (and those of other natural persons represented by them) in digital format in one of the regional health services, as well as to allow health professionals to access a set of relevant data generated in health services of other Autonomous Communities. This was intended to alleviate the problem derived from the lack of access to these data when a person traveled to another Autonomous Community in Spain.[4] Currently, the HCDSNS allows the Autonomous Communities to share relevant clinical information about their citizens so that it is available in electronic format in any regional service at the request of citizens.[5] The clinical information that can be shared is the following: Patient Summaries, known in Spain as "Historia Clínica Resumida" (HCR), that is, Summary Medical Records; Primary Healthcare Reports; Emergency Room Reports; Discharge Reports; External Surgery Reports; Laboratory Test Results Reports; Imaging Test Results Reports; Results of other Diagnostic Tests. Except for the first one, which is a document specifically created for the HCDSNS, the remaining reports already existed in the digital medical records systems of the regional services. Added to these is the possibility of communicating the EUPS (European Union Patient Summary).

In the creation and implementation of the HCDSNS, the Ministry of Health has been very aware of the work carried out by the e-Health Network[6] (in which it actively participates), in particular, in regards with the EU-Patient Summary and the EU electronic prescription and electronic dispensation projects (ePrescription/eDispensation). Taking into account the fact that the work of this network is the antecedent of the future EHDS, we can say that the HCDSNS is aligned with its objectives and, in fact, the HCDSNS aims to alleviate, on a national level, the same problems that the EHDS intends to tackle on a European level (in terms of primary use of data). In this sense, Spain is in a good starting position in order to implement the requirements regarding the primary use of data in the context of EHDS.

The priority categories of electronic health data that Member States will have to share for primary use under the EHDS are data which are already processed in the context of HCDSNS, as well as in the electronic prescription of Spanish national health system:[7] patient summaries; electronic prescriptions; electronic dispensations; medical images and image reports; laboratory results; discharge reports (Art. 5 of the Proposal[8]). This will allow the CCAA in

[3] At the regional level, the Decree 29/2009, of February 5th, which regulates the use and access to electronic medical records in Galicia, stands out. At the national level, we can highlight the Article 56 of Law 16/2003, of May 28th, on cohesion and quality of the National Health System; the Royal Decree 1093/2010, of September 3rd, which approves the minimum set of data for clinical reports in the National Health System; or the aw 41/2002, of November 14th, basic regulatory of the autonomy of the patient and rights and obligations regarding clinical information and documentation, which already contemplates the existence of medical records in electronic format, as well as the coordination of medical records on a national level by the Ministry of Health (Art. 14.2; additional provision 3rd).

[4] The background of this project is accessible at: www.sanidad.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_English.pdf .

[5] As of August 2023, the population coverage of the HCDSNS in Spain is 91%. The situational picture is accessible at: www.sanidad.gob.es/areas/saludDigital/historiaClinicaSNS/mapa/situacionActualHCDSNS.htm.

[6] This network was created based on Art. 14 of Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (accessible at: http://data.europa.eu /eli/dir/2011/24/oj).

[7] The current situation of the electronic prescription of the national health system (RESNS) can be consulted at: www.sanidad.gob.es/areas/saludDigital/recetaElectronicaSNS/home.htm.

[8] These data are described in Annex 1.

Spain (which, as has been noted, have different medical record systems) to be able to comply with the EHDS prescriptions, thanks to the works carried out in preparation for the HCDSNS and the electronic prescription system. Additionally, and as we later on explain, the HCDSNS already incorporates some of the provisions in relation to the citizens' rights regulated in the Proposal (e.g., the possibility of hiding information from the medical record from health professionals, or the access to the "access record", which we will refer to later). In this, however, the situation is more disparate at the regional level, so the CCAA will have to make an additional effort when preparing their systems for the exercise of the rights that are recognized to citizens in relation to the use of primary data in the EHDS.

2. *Provisions of the Proposal on the exchange of electronic health data for primary uses and EHR systems*

The European electronic Prescription and electronic Dispensation services and EU Patient Summary, which we have referred to in the previous section, are currently offered through the EU cross-border electronic health service infrastructure "MyHealth@EU", to which Member States are gradually being incorporated. The EHDS foresees the creation of a cross-border infrastructure for the primary use of electronic health data called MyHealth@EU (Art. 12 of the Proposal), which will clearly build on the work already carried out within the framework of the Cross-Border Healthcare Directive (Directive 2011/24/EU).[9]

In view of the Proposal, this infrastructure would consist of (Art. 12):

1) A national contact point for digital health:
   - That offers cross-border health information services for primary use (joint data controllers).
   - Under the responsibility of the States.
   - That may be established within the digital health authority designated by each State, in compliance with the Proposal.
   - To which States must ensure connection of all healthcare providers (and pharmacies).
2) A central platform for digital health:
   - Which is an interoperability platform for data exchange between the national contact points.
   - Created by the European Commission (processor).

This infrastructure will serve for the bidirectional exchange of electronic health data for the provision of healthcare; the dispensing of electronic prescriptions; but also the provision of complementary services (such as telemedicine, access by the citizens to their translated health data, exchange of health/vaccination certificates, and others).

Therefore, each Member State should designate a national contact point for digital health, who will ensure the connection to all other national contact points and the central platform for digital health. In addition, it should ensure that all healthcare providers are connected to their national contact points for digital health and that they carry out bidirectional exchanges with the national contact point. It will be the national contact point that will facilitate the exchange of personal data with the other national contact points, in the European electronic medical records exchange format, which we will refer to below.

If we look at the current status of the implementation of MyHealth@EU,[10] we see that Spain is in an advanced position in the work of implementing the Patient Summary and also, although to a lesser extent, those of ePrescription and eDispensation. This should allow for easier implementation of the provisions relating to the cross-border health infrastructure of the EHDS.[11]

However, the regulation contained in the Proposal regarding EHR systems raises more doubts. A mandatory self-certification system is established, by which these systems must demonstrate that they comply with certain essential requirements regarding interoperability and security at the European

[9] See, on the shortcomings of this Directive, J. S. Marcus, B. Martens, C. Carugati, A. Bucher and I. Godlovich, *The European Health Data Space*, IPOL | Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament Policy Department studies, 2022, 19, 20, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4300393.

[10] Available at: https://health.ec.europa.eu/ehealth-digital-health-and-care/electronic-cross-border-health-services_en.

[11] The Joint Controllership group (newly created) will approve the incorporation or disconnection of a participant from MyHealth@UE (Arts. 12.9, 66 of the Proposal).

level (Annex II). This is intended, in the words of the Proposal itself, to ensure "that electronic health records are compatible between each system and allow easy transmission of electronic health data between them". To achieve this, certain obligations regarding product conformity must be implemented: application of common conformity specifications (Art. 23); technical documentation (Art. 24); information sheet (Art. 25); EU declaration of conformity (Art. 26); and CE marking (Art. 27).

This constitutes an essential element for the correct implementation of the EHDS. Not in vain, one of the legal bases of the Proposal is Article 114 TFEU (harmonisation of the internal market). However, it is debatable whether self-certification is sufficient to guarantee citizens' rights in an area as sensitive as health data or whether a third-party conformity assessment system should be established.[12]

On the other hand, we must not forget that the legal basis of the Proposal is Arts. 16 and 114 TFEU, so we are not dealing with health policy regulations, but rather harmonization of the internal market and data protection. However, Article 168 TFEU reserves powers to the States in health policy, which constitutes a limit to the EU's action in this area. Specifically, its paragraph 7 establishes that the EU's action in public health shall respect the responsibility of States in defining their health policy, as well as the organization and delivery of health services and medical care, which includes management of health services, as well as the allocation of resources assigned to said services. Which implies that, in addition to the measures included in the Proposal constituting a genuine example of harmonization of national legislations, principles such as proportionality must also be respected. This final aspect is fundamental, taking into account the impact that the EHDS can have on the management of national medical record systems.[13] In fact, the Council is considering the introduction of a new article to clarify the freedom of States to regulate the use of wellness applications.

3. *The configuration of the patient's rights in regards to the primary use of health data*

3.1. *Rights included in the Proposal and other provisions to enforce them*

As stated at the beginning of this work, one of the main objectives of the Proposal in the field of the primary use of data is to provide individuals with greater control over the health data included in their medical records. In this sense, the Explanatory Memorandum of the text indicates that "The general objective is to ensure that natural persons in the EU have increased control in practise over their electronic health data".[14]

The original text of the Proposal opted for a novel structure, departing from what is seen in the GDPR, or in national legislations such as the Spanish one, as it did not dedicate a differentiated provision to each of the rights included; dealing with all of them in Article 3 of the Proposal. It is to be noted that the latest proposal of the Council focuses its attention on this particular matter, separating out the rights into different articles "with the aim of clarifying the scope" of each one of them.[15] However, as a new version of the articulated text incorporating these changes has not been published, references will be made to the structure of Article 3, as it is known in the original Proposal, and considering the fact that its essential content remains unchanged.

Setting this aside, it can be said that the rights included in the Proposal delimit the specific area of power that patients have over their data, in a clear attempt to provide true effectiveness to a series of rights whose application in practice has faced, to this day,

[12] This is one of the aspects highlighted in the EDPB-EDPS *Joint Opinion on the Proposal for a Regulation on the European Health Data Space*, 2022, no. 73-76 (in addition to the impact and interrelation between the declaration of conformity and compliance with data protection regulations). It is also one of the topics discussed in the Council's work, which can be consulted here:https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CONSIL:ST_9368_2023_INIT.

[13] The EDPB-EDPS *Joint Opinion* also reflects on the competence issues in relation to the legal basis of Art. 16 TFEU, raising doubts about the full compatibility of some of the provisions of Chapters II and IV of the Proposal with the law of States in the e-Health sector (in particular, the access of health professionals to restricted personal health data, the systematic registration systematic recording of the relevant health data by health.
professionals or the handle of unexpected findings by health data access bodies towards natural persons) (see, in particular, no. 14).

[14] See pp. 1, 2, 3, 5, 8, 14, 17, among others, of the Explanatory Memorandum; Recitals 1, 9, 12, 16, 67. See also the legislative financing statement attached to the Proposal.

[15] See p. 10 of the document issued by the Council, cited above.

multiple obstacles, as the Proposal itself admits.[16] In this sense, this text represents the definitive overcoming of the classic conception of personal data protection, in which the citizen acted as a mere passive spectator before the processing of their data, and their rights were not materialized, in most cases, neither from a legal point of view nor, particularly, in practice.

With this objective in mind, the Proposal takes, as a starting point, the catalog of rights already known and observable both in the data protection legislation prior to the publication of the GDPR, as well as, especially, in the latter. In this sense, it is possible to identify some classic rights, such as the right of access (paragraphs 1, 2, 3 and 10 of Article 3) or the right to rectification (paragraph 7 of the provision); while others that are somewhat more modern are also incorporated, such as the right to portability (paragraph 8), on which the Proposal insists on numerous times, from its Explanatory Memorandum.

Along with these well-known rights, the introduction of a series of provisions that can be considered as new stands out, such as the possibilities for the persons to authorise other natural persons to access their electronic health data of the person on their behalf (paragraph 5) -which appears as an obligation for Member States, who must establish services to enable this right-, to insert data into their own EHR -with indication as to whether the information has been inserted by the patient or their representative- (paragraph 6), or to restrict access to specific data (paragraph 9), among others.

Finally, within the same Article 3, there are other provisions aimed at complementing or guaranteeing the stated rights, such as the enforceability of data in electronic format (paragraph 4); provisions related to the powers of the supervisory authorities in matters of data protection regarding, specifically, these rights (paragraph 11); or a final provision, relating to the technical execution of the rights by the Commission (paragraph 12).

All of this is accompanied by the mechanisms that other parts of the Proposal provides for making these rights effective in the event of possible non-compliance or violations. This is the case, particularly, of Article 10, which introduces a new figure, the "digital health authority", responsible, as indicated in the precept, for the "implementation and enforcement of this Chapter at national level", with powers that appear to be in discordance with those provided for the supervisory authorities under GDPR, which could entail certain risks for the effective defense of the rights of natural persons.[17]

Returning to the regulation of rights done by the Proposal, it is appropriate to focus our attention on certain solutions that are particularly striking.

3.2. *The right of access: a broader scope*

The right of access to data is, as has already been said, a classic right in the matter. Observing the regulation made by Article 3 of the Proposal, some interesting points can be highglighted in relation to Article 15 GDPR and also, in regards to Spanish legislation, in Article 13 LOPDGDD (the Spanish *Ley Orgánica de Protección de Datos y Garantía de derechos digitales*, that is, the Organic Law of Data Protection and Guarantee of digital rights).

Firstly, the Proposal guarantees that the data are accessible to patients, there being a right to obtain "an electronic copy, in the European electronic health record exchange format referred to in Article 6" (paragraph 2 of the Article), of, at a minimum, the aforementioned priority categories of data collected in Article 5. But, also, this access must also be given "immediately" and "free of charge and in an easily readable, consolidated and accessible form" (paragraph 1).[18] In this

[16] It states that "Natural persons' access to their personal electronic health data remains burdensome, and natural persons have limited control over their own health data and the use of these health data for medical diagnosis and treatment" (see Explanatory Memorandum, p. 9. See also Recital 67). See also J. S. Marcus, B. Martens, C. Carugati, A. Bucher and I. Godlovich, *European Health*, 16.

[17] See the wording of Articles 3.11 and 11.1, which are clearly contradictory; or, in general, the idea, expressed in Recital 14 of the Proposal, that the supervisory authorities "must remain competent (…) to process claims submitted by natural persons", which clearly conflicts with the long list of powers conferred, according to the Proposal, to the digital health authority. In a similar sense, see EDPB-EDPS, *Joint Opinion*, no. 67, 69.

[18] In regards to the gratuity of the access to the data and the interpretation of Articles 12 and 15 GDPR, the recent CJEU ruling of 26 October 2023 (case C-307/22) confirms the right of the patient to obtain a free first copy of the medical record. The Court also elaborates on other requisites of said copy, including its intelligibility.

sense, the idea that access must be immediate is particularly noteworthy; for it is not stated in Article 15 GDPR, which is highlighted in Recital 8 of the Proposal as a circumstance that can cause significant harm to people.

However, this rule has an exception, which is that this immediate access will not occur when, in the interest of the patient, it is more advisable to wait until a health professional can "properly communicate and explain to the natural person information that can have a significant impact on his or her health" (paragraph 3). This circumstance can be easily explained considering the type of information the Article is referring to -which also justifies that this exception provision is not included in the configuration of this right in general regulations, such as the GDPR or the Spanish LOPDGDD-.

Secondly, the most remarkable aspect of the right of access' regulation -at least, from the point of view of the Spanish experience- is, without a doubt, the rule contained in paragraph 10 of the Article, which indicates that "Natural persons shall have the right to obtain information on the healthcare providers and health professionals that have accessed their electronic health data in the context of healthcare". In short, we are talking about what in Spain is known as "access to the access record"; that is, access, by patients, to the file which reflects the accesses made by professionals to their medical records.[19]

This is an issue that has been widely debated in the context of the Spanish legal system. Although access to the access record is contemplated in the HCDSNS, the applicable regulations on the matter do not respond to the specific question of whether the patients have the right to know, specifically, the identity of the professionals who accessed their data; which is a fact of radical importance, to the extent that it is likely to condition, in most cases, the protection of the rights of the injured party before the Courts.[20]

The relevance of the issue can be easily understood, especially when one sees that it raises conflicting positions in important instances. And thus, on the one hand, the Spanish data protection control authority, namely, the Spanish Data Protection Agency (Agencia Española de Protección de Datos or AEPD), has taken a stand in various resolutions and reports against the communication of this particular information.[21] The same position can be identified in different rulings,[22] some, regulations of the Autonomous Communities [23] and, although it is not expressed in an excessively-clear manner, in the explanatory document of the HCDSNS.[24]

On the other hand, the possibility of knowing the identity data of those who access the medical records is supported by different regulations of the Autonomous Communities,[25] some sentences[26] and the

[19] The "access record", in the Spanish system, is a file initially introduced by Article 103 of Royal Decree 1720/2007, of December 21st, which approves the Regulations for the development of Organic Law 15/1999, of December 13th, on the protection of personal data (that is, the data protection law in force in Spain prior to the entry into force of the GDPR), and also provided for by Article 23 of Royal Decree 3/2010, of January 8th, which regulates the National Security Scheme. It consists of a record – useful for the purposes of audits and internal controls, among others- in which every access leaves a trace of, at a minimum, the user's identification, the date and time of access, the file being accessed, the type of access, and whether it is authorized or denied. See also the details in this regard of Report 584/2009 of the Spanish Data Protection Agency.

[20] It is explained in detail in A. S. Casanova Asencio, *Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias*, in *InDret: Revista para el Análisis del Derecho*, no. 2, 2019, 18-22.

[21] See Reports 267/2005 and 171/2008 - referred, in turn, by a large number of resolutions of the same Agency (R/01999/2017, R/02324/2017, R/02410/2017, R/02411/2017, R/03001/2017, R/00970/2018, RR/00342/2018) - and the more recent Reports 0101/2019, 0098/2020 and 003/2021. The Basque Data Protection Agency stated the same position (Opinion of May 17th, 2011).

[22] Among others, the SSAN of February 26th, 2014 and February 9th, 2018 are frequently cited.

[23] See Article 19.2 of Decree 24/2011, of April 12th, on the Health Documentation of Castilla-La Mancha.

[24] The most recent document in relation to this system can be consulted here (see pp. 16, 38, 45, 47 *et seq*., where it can be noted that the data related to the identity of the person accessing is not included in the information that the patients can consult through this service, also indicating that this information is registered - apparently, solely - for audit purposes): www.sanidad.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_English.pdf.

[25] See Arts. 31.1. of the Foral Law 17/2010, of November 8th, on the Rights and Duties of People in matters of Health of the Autonomous Community of Navarra and 35.3 of Law 3/2005, of July 8th, on Health Information and Autonomy of the Patient from the Autonomous Community of Extremadura.

[26] One recent and worthy to be highlighted example is the STS, Chamber 2, of 25 September 2020, to which the AEPD expressly refers, although with a somewhat surprising interpretation, in its Report 003/2021.

generality of Spanish doctrine,[27] in addition to other entities, both national[28] and international -as is the case, notably, of the Article 29 Working Part (current European Data Protection Board)[29]-.

Aside from the arguments put forward in favor of one position or the other, the regulation of the Proposal on this point represents a decisive support for the position in favor of access to these data; which, if the text materializes in a Regulation, would undoubtedly lead to a change in the doctrine of the Spanish AEPD. All things considered, it is also the most favorable solution in regards to the promotion of the rights of patients, in line with the general objectives of the Proposal; reason for which it has to be judged favorably.[30]

3.3. *Medical records: between a basic tool for healthcare and the personal data spaces*

Some of the rights contained in Article 3 of the Proposal are in clear connection with the idea that the EHR is a data space over which the patient has an important scope of decision, and can partially configure it, in connection with certain initiatives carried out in certain States of the European Union.[31]

This is the case, mentioned above, of the possibility of data insertion by the patient; of the right of rectification, of which Article 3 of the Proposal provides only a brief overview, to refer, generically, to the GDPR (paragraph 7); or, in a particularly problematic provision, the right that the patient would have to "restrict access of health professionals to all or part of their electronic health data" (paragraph 9).

This last issue had been debated for some time in different forums;[32] in particular, regarding particularly sensitive health data, such as those related to infectious diseases, mental health data, voluntary terminations of pregnancy,[33] and others. Singularly, it had been raised by the Article 29 Working Party - which, among different options to articulate this right, discussed whether there should be a notice regarding the presence of this hidden data;[34] an idea that, on the other hand, has been criticised both by the Spanish doctrine[35] and by the AEPD.[36]

The system introduced by the Proposal implies that the professional cannot access the data unless there is express authorization from the patient, "including where the provider or professional is informed of the existence and nature of the restricted electronic health data",

[27] S. Gallego Riestra and I. Liano Galán, *¿Tiene derecho el paciente a saber quiénes y por qué han accedido a su historia clínica?*, in *Derecho y Salud*, vol. 2, no. 1, 2012, 88, 89; L. González García, *Derecho de los pacientes a la trazabilidad de los accesos a sus datos clínicos*, in *Derecho y Salud*, vol. 24, no. 1 extra, 2014, 279-281; S. Gallego Riestra, *Los derechos de acceso, rectificación, cancelación y oposición del paciente a su historia clínica*, in *Derecho y Salud*, vol. 26, no. 1 extra, 2016, 137-139; or in A.S. Casanova Asencio, *Protección de datos*, 14 et seq. (in particular, 18 et seq.), recently supported, expressly, by I. Alkorta Idiakez, *El Espacio Europeo de Datos Sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2022, 55.

[28] Spanish Society of of Public Health and Health Administration (SESPAS: Sociedad Española de Salud Pública y Administración Sanitaria), *Protection of personal data and professional secrecy in the field of health: a regulatory proposal for adaptation to the GDPR*, (originally, in Spanish, "Protección de datos personales y secreto professional en el ámbito de la salud: una propuesta normative de adaptación al RGPD"), Spain, 2017, 65, 66, accessible here: http://sespas.es/2017/11/30/proteccion-de-datos-personales-y-secreto-profesional-en-el-ambito-de-la-salud-una-propuesta-normativa-de-adaptacion-al-rgpd. See also the nuances indicated in A.S. Casanova Asencio, *Protección de datos*, 17, footnote no. 50.

[29] Working Document on the processing of personal data relating to health in electronic health records (EHR) (Document WP131), 2007, 21 (hereinafter, Document WP131). Accessible here: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp131_en.pdf

[30] In the same sense, EDPB-EDPS, *Joint Opinion*, no. 58.

[31] This is the case, singularly, of the *Personal Digital Healthcare Environment* of the Netherlands (*see,* in this regard, by I. Alkorta Idiakez, *Espacio Europeo*, 19)

[32] In favor, with limits, SESPAS, Protection of personal, 53, 54; J. Sánchez Caro, *La historia clínica gallega: un paso importante en la gestión del conocimiento*, in *Derecho y Salud*, vol. 18, no. 1, 2009, 70.

[33] The Spanish Organic Law 2/2010, of March 3rd, on sexual and reproductive health and voluntary interruption of pregnancy, provides for specific measures in relation to this issue; some of which have been subject to recent reform, furthermore, by virtue of Organic Law 1/2023, of February 28th, which modifies, among others, Articles 20 and 23 of the 2010 Law.

[34] Document WP131, p. 14.

[35] SESPAS, *Protection of personal*, 54; J. Sánchez Caro, *La historia clínica*, 70; J. Etreros Huerta, *Historia clínica electrónica*, in R. Cáliz Cáliz (coord.), *El derecho a la protección de datos en la historia clínica y la receta electrónica*, Cizur Menor (Navarra), Thomson Reuters Aranzadi, 2009, 181 (especially, 190); A.S. Casanova Asencio, *Mecanismos de prevención del acceso indebido a la historia clínica por parte del personal sanitario y nueva legislación de protección de datos*, in *Bioderecho.es: Revista internacional de investigación en bioderecho*, no. 7, 2018, 11.

[36] Report 656/2008.

as indicated in Article 4.4.

Patients' mandatory authorization can only be bypassed, as an exception, when there is a risk to the vital interests of the patient or another person, in which case the data may be accessed, subsequently informing the interested party and other subjects indicated by the precept. In this sense, we cannot ignore the fact that the right in question can pose a significant risk to both the life and health of patients and that of third parties, including health professionals themselves.[37]

The addition of this exception is palpable proof of the awareness of the important potential risks derived from the exercise of this right, with the Proposal warning that the natural person who opts for the unavailability of health data must "assume responsibility for the fact that the healthcare provider cannot take the data into account when providing health services" which is quite significant.[38]

This provision, moreover, leaves a good number of questions unresolved. Thus, it does not specify aspects such as whether all the data contained in the medical records could be hidden;[39] if, as stated above, there would be some type of notice to the health professionals regarding the presence of hidden data;[40] or if discrimination could be made in regards to specific professionals, professional categories, or, also, specific types of data.[41] Certainly, the formulation used by the Proposal is fairly brief on this point; noting that it refers to national regulations for the purposes of establishing "the rules and specific safeguards regarding such restriction mechanisms", which may favor a particularism somewhat contrary to the objectives of the Proposal itself.

In relation, precisely, to the national configuration of this measure, it can be remarked that this option is already included, in the case of Spain, in the HCDSNS, where the concealment of clinical reports and documents is allowed, after the display of a notice about the risks involved in exercising this right, and as a solution that may be "reversed by the user at any time".[42]

What is even more relevant: it is provided that the professional "will be informed of the existence of hidden information (without specifying what kind of information it is) so that, if knowing all the information were so important in the specific clinical context, the patient may understand the convenience of revealing the non-visible contents after having been duly informed". And, in addition, it is also foreseen that protected information can be accessed in the event of an "emergency situation requiring urgent action", when the patient is not in a position to give consent, although then "an audit trail indicating both circumstances" would be left.[43]

4. *Concluding remarks*

Once the preceding analysis has been made, it is worth considering that the rights of natural persons regarding primary use of their data are developed,[44] and even expanded,[45]

[37] It could be criticised that the limit relating to the rights of third parties is only applicable when the "vital interests" of said third parties are at stake, and not simply their right to health, resulting to be an excessively lax limit. Furthermore, this idea may encounter obstacles in practice, if health professionals are unaware of the existence of the data; especially, if the patient is not in a position to communicate this circumstance.

[38] Furthermore, it is indicated that "these restrictions may have life-threatening consequences and, therefore, access to personal electronic health data must be possible to protect vital interests in the event of an emergency", in addition to specifying what should be understood by "vital interest" (Recital 13). This would undoubtedly have an impact on the liability that would correspond to health professionals who do not administer a treatment, or administer an incorrect treatment, due to lack of necessary data in the evaluation of the patient's condition; which could then be significantly reduced or even completely eliminated.

[39] Certainly, the text of the Proposal does not establish a limit in this regard, and the Article 29 Working Party raised it as a possibility (*Document WP131*, 14). See also I. Alkorta Idiakez, *Espacio Europeo*, 61, 62.

[40] No specific statement on this regard can be found in the Proposal, while the wording used in the Article isn't particularly conclusive.

[41] The option of restricting the data regarding specific individuals who could have access to the medical records and have a previous relationship with the patient has been raised; as well as the possibility to discriminate depending on the professional category of the person accessing; or, similarly, the possibility of restricting access to data other than clinical data - thus, identifying data - (see A. S. Casanova Asencio, *Mecanismos de prevención*, 12-14; AEPD Report 0054/2010).

[42] See p. 17 of the explanatory document of HCDSNS, linked above.

[43] See p. 18 of the explanatory document of HCDSNS, linked above.

[44] According to the Explanatory Memorandum of the Proposal, its Chapter II, which is aimed at strengthening and promoting the control of natural persons over their own data, "develops the additional rights and mechanisms designed to complement the natural person's rights provided under the GDPR in relation to their electronic health data" (p. 18).

[45] In the same sense, R. Martínez Martínez, *Digitalización y construcción normativa de los Espacios Europeos de Datos. Retos para el sector público. Los*

through an application to the context of health data, which responds to the specific nature of the Proposal, in contrast with the general scope of the GDPR.[46]

In general, the proposed solutions are clearly aimed at seeking the announced strengthening of natural persons' control over their data,[47] which, on many occasions, serves to respond to questions that had been consistently raised in view of current regulations. And, what is more, some of them can be clearly controversial, as has been explained.

In any case, what seems obvious is that the configuration of the rights presented in the analysed Proposal will have a decisive influence, if it ends up being approved as a regulation, on the way in which the management of national medical records systems is structured.[48] In this sense, it is worth noting that medical records have traditionally been considered only as a tool or instrument at the service of health personnel for the provision of health care;[49] which is very far from the conception that presides over both the Proposal and the European Data Strategy, in which we would be faced with personal data spaces over which patients would have broad configuration powers.

Therefore, it seems clear that the development of this Strategy will require a reform of national legislations such as the Spanish one, either to restructure the already-existing medical record services, so that they can comply with the requirements derived from the European Health Data Space, or to create data spaces independent of national electronic medical records, in connection with the obligation for Member States provided for in Article 3.5.a) to establish electronic health data access services that allow the exercise of the rights enshrined in the precept.

On top of this, the implementation of the cross-border infrastructure for the primary use of data within the EU will be more or less complex depending on the specific state of preparation of each of the countries where it must be implemented. In the case of Spain, it should not entail excessive problems, to the extent that the HCDSNS system is planned, as has been said, to alleviate -at the national level, and with the territorial particularities of Spain- problems similar to those noticeable in the sharing of data for primary use between the different Member States of the Union. Furthermore, it is pertinent to remember that the e-Health Network has been a clear reference for the implementation of the HCDSNS.

Likewise, it has also been indicated that Spain is advanced in the implementation work of the Patient Summary, ePrescription and eDispensation. In contrast, the self-certification scheme for EHR systems generally raises more doubts, which must be resolved, both because of its relevance in relation to the protection of citizens' rights, and because of the impact that these measures are likely to generate in the internal legal systems of the Member States upon their implementation.

datos de salud, in *La Ley Privacidad*, no. 13, 2022, 5; see also S. Navas Navarro, *Datos sanitarios electrónicos. El espacio europeo de datos sanitarios*, Madrid, Reus, 2023, 117.
However, see also L. Marelli *et al*., *The European health data space: too big to succeed?*, in *Health Policy*, no. 135, 2023, 2, available at: www.sciencedirect.com/science/article/pii/S016885102300146X.

[46] In the same sense, EDPB-EDPS, *Joint Opinion*, no. 19, 47, 50, which also addresses the coordination problems that may arise, regarding the rights of natural persons, between these two texts; see also D. Horgan, M. Hajduch, M. Vrana, J. Soderberg, N. Hughes, M. I. Omar, J. A. Lal, M. Kozaric, F. Cascini, V. Thaler *et al*, *European Health*, 1629.

[47] Always in the context of the primary use of the data, which stands out in comparison with the treatment of secondary use of data, in regards to which the rights of natural persons are not defined (see M.B. Andreu Martínez, *Datos de salud y bien común: hacia la construcción de un mercado europeo de datos sanitarios*, in M. B. Andreu Martínez and A. Espinosa de los Monteros Rodríguez (coord.), *Tecnología para la salud: una visión humanista desde el Bioderecho*, Madrid, Plaza y Valdés Editores, 2023, 236), which has been heavily criticised (EDPB-EDPS, *Joint Opinion*, no. 35; European Digital Rights (EDRi), *Make the European Health Data Space serve patients and research*, 2023, 3, accessible here: https://edri.org/wp-content/uploads/2023/03/EHDS-EDRi-position-final.pdf), conforming one of the matters on which the Council has suggested important changes (see p. 10 of the explanatory document, linked above).

[48] See, for instance, the data collected regarding the implementation of electronic medical records in different EU countries (among others, Belgium, Netherlands, Portugal, Estonia, Germany, The Netherlands, Spain and Finland) in J. S. Marcus, B. Martens, C. Carugati, A. Bucher and I. Godlovich, *European Health*, 26, 27.
See also L. Marelli et al, *European Health*, 2.

[49] In the case of the Spanish legislation, it is identified, not in vain, as "an instrument fundamentally intended to guarantee adequate care to the patient" (Art. 16.1 of the aforementioned Law 41/2002, of November 14th, on patient autonomy).

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 187-200
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 14

*The Italian Electronic Health Record (EHR)**

Nicola Posteraro
(Associate Professor in Administrative Law at University of Milan)

Stefano Corso
(Research fellow, PhD in Private Law at University of Padua)

ABSTRACT The work analyses the Italian legislation governing the electronic health record (EHR). Among the other things, it dedicates particular attention to the role of this tool in the context of the Italian healthcare digitalisation; the paper also deals with the problems related to the elimination of the data subject's consent for the implementation of the EHR and it tries to highlight some possible actions for the enhancement of this tool expressly provided by the Italian National Recovery and Resilience Plan (NRRP).

1. *The Electronic Health Record (EHR) as a tool of Italian digital health*

The *Electronic Health Record* (EHR) holds a central role among Italian e-Health tools: it is 'a pillar' within the initiatives related to the pathway towards digital health and it constitutes the main enabling factor for the achievement of significant improvements in the quality of services provided in the health sector.[1]

The EHR is a digital collection of all health and socio-medical data and documents relating to a person's medical history and it is part of the broader process of dematerialisation/transfer of health records into digital format.[2] More specifically, it is an "archive of the health of the patient", which, set up by the respective Italian Regions (and Autonomous Provinces),[3] is implemented over time by the practitioners of the health professions and by the patients themselves.[4] In this sense, it is one of the clearest manifestations of the culture whereby architecture is designed to fully serve the interaction between health professionals and between patients and doctors.

At the legislative level, the EHR was officially introduced in Italy in 2012;[5] however, even before the instrument acquired "national" importance, several regions had already started project activities for the implementation of EHR systems at local levels.

The main purpose of the EHR is to create an organic information base, with continuous implementation, that favours the improvement of prevention, diagnosis, treatment and rehabilitation of patients.[6]

It enables the digital sharing of health data and documents created, integrated and updated over time by several parties; it is thus able to document patients' entire medical history, report their several health events and offer a better care process.

Thanks to the EHR, patients can trace and consult the entire history of their health life, sharing it with health professionals in order to obtain a (at least abstractly) more effective and more efficient service: it is evident, for instance, that the tool provides a valid support for the continuity of care, as it allows the

---

[*] Article submitted to double-blind peer review.
The work is a joint study of the two authors; specifically, N. Posteraro is the author of paragraphs 2, 5, 8 and 9, while S. Corso is the author of paragraphs 3, 4, 6 and 7. Paragraph 1 was written by both the authors.

[1] This is the description of the EHR found on the official website: *www.fascicolosanitario.gov.it.*

[2] A process that, in Italy, was launched in 2011 with the aims of implementing the true potential of data collected, cutting the costs of managing and archiving "paper", streamlining and speeding up procedures; over time, it has also involved medical records, prescriptions and reports. N. Posteraro, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *www.federalismi.it*, 17 November 2021.

[3] The Italian EHR is therefore a model whose infrastructure is based on a national network of regional/provincial architectures (also for this reason, it is different from the English and French models, designed respectively with a mixed and centralised architecture at national level).

[4] Article 12(3) of d.l. No. 179 of 18 October 2012 (the so-called "Decreto crescita", later converted into Law No. 221 of 17 December 2012).

[5] More specifically, by Article 12 of d.l. No. 179 of 18 October 2012.

[6] See Article 12(2)(a) and (a-*bis*) of d.l. No. 179/2012; P. Guarda, *Fascicolo Sanitario Elettronico e protezione dei dati personali*, Trento, Università degli Studi di Trento, 2011, 26.

various professionals who are already in charge of a patient to be aware of the diagnostic and therapeutic initiatives carried out by their colleagues. In this sense, the EHR contributes to create an e-Health system based on the centrality of the patient.[7]

Clearly, the possibility of retracing the history of a clinical pathway is highly dependent on the fact that all the documents contained in the EHR, in addition to being easily retrievable, are correctly stored and protected from modification or alteration. This is a particularly important issue, if we consider not only that there has been a dangerous exponential increase in cyber-attacks aimed at stealing numerous health data in our country in recent years, but also that, as things stand, there is still little awareness on the part of healthcare facilities of their obligation, as data controllers, to adopt logical security measures aimed at protecting their computer systems and, consequently, the integrity of the data.[8]

The purposes of diagnosis, treatment and rehabilitation of patients are pursued by the subjects of the National Health Service (NHS) and the regional socio-health services and by all health professions;[9] those of prevention, on the other hand, are pursued (in addition to the subjects of the NHS and the regional socio-health services and by the health professions) also by the offices of the Regions and Autonomous Provinces responsible for preventive health care and by the Ministry of Health.[10]

Added to these purposes are those of international prophylaxis, pursued by the Ministry of Health.[11]

At the same time, the EHR also acts as a support for the study and the scientific research in the medical, biomedical and epidemiological fields, as well as for health planning, quality of care verification and health care evaluation.[12] For the sake of completeness, it should be pointed out that, under the current legislation, the subjects deputed to achieve the above-mentioned purposes,[13] within the limits of their respective competences attributed by law, may access the file and process the data contained therein, provided that they are deprived of identifying elements, on the assumption that, for these purposes, other than those of prevention and personal care, it is sufficient to use non-identifying information.

In this sense, the regulation of the EHR (the establishment of which therefore gives rise to a further processing of personal data, distinct from all the processing deriving from the provision of health services to the patient in relation to which the data have been acquired or produced) constitutes an emblematic application of the delicate balance

[7] The EHR is different from the Electronic Medical Record because: whereas the EHR describes the patient's entire clinical life, the electronic medical record (which can be defined as a digital document created by the healthcare facility treating a patient in order to manage his or her clinical data and to guarantee continuity in care pathway) only refers to a single episode of hospitalisation of the person concerned. However, it seems appropriate to point out that the electronic medical record also differs from the health record which collects all the clinical information relating to all the operations performed for the patient in the facility that receives him or her (and thus serves to make the processes of diagnosis and treatment of the patient within a single health facility more efficient). See A. Thiene, *Salute, riserbo e rimedio risarcitorio*, in *Rivista italiana di medicina legale*, 2015, 1421; L. Califano, *Fascicolo sanitario elettronico (EHR) e dossier sanitario: il contributo del Garante Privacy al bilanciamento tra diritto alla salute e diritto alla protezione dei dati personali*, in G. de Vergottini and C. Bottari (eds.), *La sanità elettronica*, Bologna, Bononia University Press, 2018, 29; A. Pioggia, *Il Fascicolo sanitario elettronico: opportunità e rischi dell'interoperabilità dei dati sanitari*, in R. Cavallo Perin (ed.), *L'amministrazione pubblica con i* big data*: da Torino un dibattito sull'intelligenza artificiale*, Torino, Università degli Studi di Torino, 2021, 216.

[8] Cf. E. Sorrentino and A.F. Spagnuolo, *La sanità digitale in emergenza Covid-19. Uno sguardo al fascicolo sanitario elettronico*, in *Federalismi*, 2020, as well as the data released by the Agency for Digital Italy (AGID) in the Report on ICT Expenditure in Italian Territorial Healthcare - *www.agid.gov.it/sites/default/files/repository_files/rapporto_agid_sulla_spesa_ict_nella_sanita_territoriale*). In this regard, it should be noted that, as pointed out by AGID, the Italian Public Administration more generally lacks awareness of the threat and notes the absence of local-organisational structures capable of effectively operating an incident preparation and response activity (see on this point the Three-Year Plan for Information Technology in Public Administration 2019-2021, in which the Agency has retraced some important criticalities that emerged in the Report "Italian Cyber Security Report 2014"). On this point, it should be noted that, according to the 2018 Clusit report, in the public sector in general, attacks have increased by 41%, reaching a peak of 99% in the health sector (*https://ofcs.report/wp-content/uploads/2019/03/Rapporto_Clusit_2019.pdf*) and, in the 2021 report, the growth of attacks in the health sector continues to be highlighted.

[9] Article 12(4) of d.l. No. 179/2012.

[10] Article 12(4-*bis*) of d.l. No. 179/2012.

[11] Article 12(2)(a-*ter*) and 12(4-ter) of d.l. No. 179/2012, introduced by d.l. No. 4 of 2022.

[12] Article 12(2)(b) and (c) of d.l. No. 179/2012.

[13] The Regions, the Autonomous Provinces, the Ministry of Labour and Social Policy and the Ministry of Health.

between the principle of the free circulation of data, functional to the protection of public health and the requirements of administrative efficiency, and the right to privacy, paramount to safeguard the personal dignity.[14]

The EHR, then: a) ensures undoubted advantages in terms of lightening the burden of documentation (and, therefore, considerable savings in time and expense); b) provides effective support for management and administrative activities related to care processes (as it allows, for example, administrative information such as bookings for specialist visits, prescriptions, etc., to be shared between operators); c) allows a significant reduction in medical errors (the doctor knows the patient's clinical situation in greater detail, before intervening); d) prevents health professionals from prescribing examinations that would prove unnecessary because they have already been carried out, with a consequent reduction in treatment times and an inevitable decrease in the costs that the widespread phenomenon of so-called defensive medicine actually produces in our country.

2. *Some innovations made in 2020 to the EHR regulation*

In 2020, the legislator extended the database of the HER:[15] it now also includes information on private services provided outside the NHS whose recording on patients' personal handbooks was previously left to their discretion. This is an important change, given that the care provided outside the NHS constitutes a significant part of the healthcare services, in Italy, and that, in the face of such exclusion, the patients' medical history often risked being only half known by those who had to take care of them. The reasons were mainly twofold: on the one hand, not every patient had the possibility to insert such information in his or her personal-notebook area -see *infra*-, which was often missing, since it was not envisaged by the reference Region/Autonomous Province among the so-called supplementary elements of the EHR. On the other hand, not all the patients who could make such an entry actually did so, either because they were digitally incompetent, or because they forgot, or because they had little knowledge of the tool, and/or because they were not duly informed of the possibility of actively participating in the enrichment of the information. The legislator's aim is clearly to enhance the effectiveness of the EHR by broadening the type of information processed.

The legislator then revised the rules for the implementation of the record, stipulating that it is no longer dependent on patients' free and informed consent, but rather it becomes automatic.[16] In other words, once the EHR has been activated, patients' data on their use of healthcare services will automatically be included in the digital collection.[17]

The amendment seems to give continuity and completeness to the health database: in this way, the governance and research purposes, summarily mentioned above, may perhaps be more adequately achieved (they would otherwise be -and have been so far- pursued through the processing of potentially-incomplete data).[18]

However, it will certainly be necessary to understand to what extent such an innovative context is compatible with today's legal framework for the protection of personal data: for example, it will have to be ascertained whether this type of processing -not permitted- is compatible with the GDPR, given that, pursuant to Article 9(1), it is

[14] See S. Corso, *Il fascicolo sanitario elettronico fra e-Health, privacy ed emergenza sanitaria*, in *Responsabilità Medica,* 2020, 396; A.M. Gambino, E. Maggio and V. Occorsio, *La riforma del fascicolo sanitario elettronico*, in *Diritto Mercato Tecnologia*, 2020, 2. On the impact of technology in the structures of contemporary society, see G. Biscontini *et al*., *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *www.federalismi.it*, 2020; A.G. Orofino, *La semplificazione digitale*, in *Il diritto dell'economia*, No. 3, 2019, 87-112, and on the related concept of risk, A. Barone, *Il diritto del rischio*, Milano, Giuffrè, 2006.

[15] The amendments were made by d.l. No. 34 of 19 May 2020, converted, with amendments, by Law No. 77 of 17 July 2020.

[16] In particular, Article 12(3-*bis*), d.l. No. 179/2012, stated: "The EHR may be fed exclusively on the basis of the free and informed consent of the patient, who may decide whether and which data relating to his or her health should not be included in the file itself". See S. Bologna et al, *Electronic Health Record in Italy and Personal Data Protection*, in *European Journal of Health Law*, No. 23, 2016, 265 ff. This paragraph was repealed by Article 11(1)(d) of d.l. No. 34 of 19 May 2020, converted, with amendments, by Law No. 77 of 17 July 2020.

[17] This is made explicit in the updated summary sheet available on the institutional website of the GPDP, aimed at summarising the new regulations. This is the infographic of 19th June 2020, *Le novità sul FSE*, available at *www.garanteprivacy.it.*

[18] And the same applies now for international prophylactic purposes.

forbidden to process, inter alia, data relating to the health of the individual.[19] Article 9(1) of the GDPR prohibits the processing of, inter alia, data relating to a person's health; it may indeed be argued that, in such cases, one of the hypotheses set out in Article 9(2) is relevant, which is capable of derogating from the aforementioned general rule prohibiting the processing of data relating to an individual's health; however, it will always remain to be ascertained whether, in order to achieve the purposes envisaged by those hypotheses deemed applicable, the processing thus carried out is really "necessary".[20]

3. *The problem of consent*

The decision to overcome the consent requirement is in line with the statements of the Italian Data Protection Authority, which, in its provision No. 55 of 7 March 2019,[21] admitted the possible elimination of the need to acquire the data subject's consent to the feeding of the record.

The Authority's position was based on the renewed regulatory framework, following the entry into force of the General Data Protection Regulation and Legislative Decree No. 101 of 2018, adjusting the provisions contained in Legislative Decree No. 196 of 2003, the Italian Privacy Code.

The prohibition on the processing of particular categories of personal data, including data relating to health,[22] set out in Article 9(1) of the Regulation[23] is waived in the cases listed in paragraph 2 of the same article. Of these, consent is only one of the exceptions.

The processing of health data,[24] in particular, is not prohibited if it is «necessary for reasons of substantial public interest, on the basis of Union or Member State law [...]» (g); «necessary for the purposes of [treatment] [...]» (h); «necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices» (i); or necessary for the purpose of scientific research (j).[25]

[19] For example, one could refer to letter i) of paragraph 2 of the aforementioned Article 9 of the GDPR, expressly referred to by Art. 75 of the Italian Privacy Code, according to which processing is lawful if it is "necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products and medical devices, on the basis of Union or Member State law that provides for appropriate and specific measures to protect the rights and freedoms of data subjects, in particular professional secrecy"; but one may also consider applicable letter g) of the above-mentioned paragraph 2 of Art. 9 of the GDPR, according to which processing is permitted if it is "necessary for reasons of substantial public interest on the basis of Union or Member State law, which must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for appropriate and specific measures to protect the fundamental rights and interests of the data subject". That letter g) may be relevant with regard to the processing of data contained in the EHR has recently been confirmed by Law No. 205 of 3 December 2021, converting, with amendments, d.l. No. 139 of 8 October 2021, which introduced, in Article 2-sexies of the Privacy Code, paragraph 1-*bis*.

[20] It is unclear what meaning should be attached to the adjective "necessary": see paragraph 5.

[21] See F.G. Cuttaia, *The impact of EU Regulation 2016/679 on the Italian health system*, in G. Fares (ed.), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analy*sis, Torino, Giappichelli, 2021, 195 ff., especially 200; S. Corso, *Sul trattamento dei dati relativi alla salute in ambito sanitario: l'intervento del Garante per la protezione dei dati personali*, in *Responsabilità medica*, 2019, 236.

[22] It is just worth mentioning that Directive No. 46 of 1995 did not define health data, but in 2003, the Court of Justice gave it a broad interpretation, in relation to Article 8(1) of the Directive, in the famous "Lindqvist" case. ECJ EU, 6 November 2003, Case C-101/01 (*Lindqvist*), in *Europa e diritto privato*, 2004, 1001 ff., with a note by R. Panetta, *Trasferimento all'estero di dati personali e Internet: storia breve di una difficile coabitazione*. As is well known, now, EU Reg. No. 679 of 2016 defines health-related data in Art. 4(15) as «personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status». See L.A. Bygrave and L. Tosoni, *sub* art. 4(15), in C. Kuner, L.A. Bygrave and C. Docksey (eds.), *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford, Oxford University Press, 2020, 217 ff. See also W. Schäfke-Zell, *Revisiting the definition of health data in the age of digitalized health care*, in *International Data Privacy Law*, vol. 12, No. 1, 2022, 33 ff.; A. De Franceschi, *sub* art. 4, in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta (eds.), *Codice della privacy e* data protection, Milano, Giuffrè, 2021, 156 ff.

[23] L. Georgieva and C. Kuner, *sub* art. 9, in C. Kuner, L.A. Bygrave and C. Docksey (eds), *The EU General Data Protection Regulation (GDPR)*, 365 ff.; A. Thiene, *sub* art. 9, in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta (eds.), *Codice della privacy e* data protection, 240 ff.

[24] For an analysis of various specific profiles relating to the processing of health data, see A. Thiene and S. Corso (eds.), *La protezione dei dati sanitari. Privacy e innovazione tecnologica tra salute pubblica e diritto alla riservatezza*, Napoli, Jovene, 2023; C. Perlingieri, *eHealth and Data*, in R. Senigaglia, C. Irti, and A. Bernes (eds.), *Privacy and Data Protection in Software Services*, Berlin, Springer, 2022, 127 ff.

[25] I. Rapisarda, *Ricerca scientifica e circolazione dei dati personali. Verso il definitivo superamento del para-*

In relation to the processing of personal data in the health sector, Article 75 of the Privacy Code now provides that «the processing of personal data carried out for the purpose of protecting the health and physical safety of the person concerned or of third parties or the community must be carried out in accordance with Article 9(2)(h) and (i) and (3) of the Regulation, Article 2-septies of this Code, and in compliance with the specific provisions of the sector».[26]

To this must be added what is now set forth in Article 2-*sexies*(1-*bis*) of the Privacy Code, introduced by Law No. 205 of 3 December 2021, converting, with amendments, d.l. No. 139 of 8 October 2021, containing "Urgent provisions for access to cultural, sporting and recreational activities, as well as for the organisation of public administrations and in matters of personal data protection" ("Decreto Capienze"). This provision expressly allows institutional subjects' the processing of data relating to health, without direct identification elements, for reasons of relevant public interest, i.e. pursuant to Article 9(2)(g) of the Regulation, including EHR data.

The relevant public interest, as well as the public interest in the area of public health, thus seems to act as an opening valve – also in view of the broad scope of the list of matters in which the public interest is deemed relevant in Article 2 sexies(2) – almost like a general clause, which essentially eliminates the prohibition of treatment, when the general public element occurs.

It must be said, moreover, that for a long time, perhaps even since the dawn of reflection on data protection, light has been shed on the inconsistency of considering data subjects' consent to processing as a control instrument in the circulation of data. In fact, it has been highlighted how consent is most often given without any awareness, with carelessness. And that data subjects are often unable to understand what they are consenting to, even when they try. And, furthermore, if they do understand, the choice to consent comes to be constrained, because otherwise the service connected to the processing will not be provided. Consent has come to be spoken of in terms of a "paradox". All this perhaps takes on even more marked traits in the healthcare context, if we consider that there can be no healthcare treatment in the absence of the processing of data relating to the patient's health by the doctor.[27]

Consent, therefore – to use Stefano Rodotà's words – is a "myth"[28] or a semblance of protection, at least consent understood in the sense of a legal basis for the legitimacy of personal-data processing.[29]

In order to offer protection to the person,[30] by guaranteeing the protection of personal data – especially sensitive data – other instruments, other than consent, have therefore been sought. And the choice has fallen on a series of measures and expedients, mainly of a technical nature, which have then been translated into principles and rules and which can, to a large extent, be said to be included in the concept of "security".[31]

Think of the principle of accountability,[32]

digma privatistico?, in *Europa e diritto privato*, 2021, 301 ff.; A. Bernes, *La protezione dei dati personali nell'attività di ricerca scientifica*, in *Nuove leggi civili commentate*, 2020, 175 ff.

[26] M. Di Masi, *sub* art. 75, in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta (eds.), *Codice della privacy e* data protection, 1233 ff.; F. Zanovello, *sub* art. 2-*septies*, *ivi*, 1051 ff.

[27] G. Finocchiaro, *Il trattamento dei dati sanitari: alcune riflessioni critiche a dieci anni dall'entrata in vigore del Codice in materia di protezione dei dati personali*, in G.F. Ferrari (ed.), *La legge sulla privacy dieci anni dopo*, Milano, Egea, 2008, 213. See also J. Hansen *et al.*, *Assessment of the EU Member States' rules on health data in the light of GDPR*, Luxembourg, Publications Office of the European Union, 2021, 28.

[28] S. Rodotà, *Elaboratori elettronici e controllo sociale*, Bologna, il Mulino, 1973, 45 ff. See also G. Buttarelli, *Banche dati e tutela della riservatezza. La privacy nella società dell'informazione. Commento analitico alle leggi 31 dicembre 1996, nn. 675 e 676 in materia di trattamento dei dati personali e alla normativa comunitaria ed internazionale*, Milano, Giuffrè, 1997, 377.

[29] A. Gentili, *La volontà nel contesto digitale: interessi del mercato e diritti delle persone*, in *Rivista trimestrale di diritto e procedura civile*, 2022, 701 ff., especially 704.

[30] The ultimate goal of all privacy legislation. For all, see P. Perlingieri, *Il diritto civile nella legalità costituzionale secondo il sistema italo-europeo delle fonti*, III, *Situazioni soggettive*[4], Napoli, Edizioni Scientifiche Italiane, 2020, 1 ff.; Id., *La persona e i suoi diritti. Problemi del diritto civile*, Napoli, Edizioni Scientifiche Italiane, 2005, and, Id., *La pubblica amministrazione e la tutela della* privacy. *Gestione e riservatezza dell'informazione nell'attività amministrativa*, *ivi*, 255 ff.

[31] See G. Finocchiaro*, Il quadro d'insieme sul Regolamento europeo sulla protezione dei dati personali*, in G. Finocchiaro (ed.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Bologna, Zanichelli, 2017, 1 ff.

[32] C. Camardi, *Liability and Accountability in the 'Digital' Relationships*, in R. Senigaglia, C. Irti and A. Bernes (eds.), *Privacy and Data Protection in Software Services*, 25 ff.; M.G. Stanzione, *La protezione dei dati personali tra «consumerizzazione» della privacy e prin-*

or the notions of privacy by design and privacy by default or pseudonymisation procedures and risk-assessment mechanisms.[33]

Security, therefore, as an obligation of the subjects, data controllers and processors.[34]

Nevertheless, with regard to the processing of health data by means of the EHR, some doubts about interpretation seem to remain.

Looking at the wording of Article 9 of the Regulation, it can be seen that the exceptional cases referred to in paragraph 2, which derogate from the prohibition expressed in paragraph 1 and which come into play in relation to the processing of data relating to health by means of the EHR, are constructed as cases for "necessary" processing. The principle of necessity, which undoubtedly also applies to the processing of so-called neutral or common data, as expressed in Article 6 of the Regulation, a fortiori applies with reference to the processing of sensitive data. Now, how the adjective "necessary" is to be understood can be debated. One might think that "necessary" means "useful" or "functional": when the processing of sensitive data is useful in the cases listed in Article 9(2), then it is not prohibited. Or one might think that "necessary" stands for "indispensable", i.e. the processing of sensitive data is not prohibited when it is indispensable for the purpose set out in the cases listed in paragraph 2 and cannot be done otherwise. However, of the two interpretations, the more convincing seems to be the second,[35] since accepting the first would deprive the prohibition set out in paragraph 1 of any real meaning - not merely emphatic: in fact, which processing of personal data does not appear useful, which is not necessary to better achieve one of those purposes? The exception would become the rule.[36]

If, however, one accepts the second interpretation, i.e. that the prohibition is only waived when the processing of data is indispensable – in this sense necessary – can it then be argued that the processing of health data by means of the EHR is the only possible way of responding to the public interests in the field of health, as indicated by law? If the answer is in the affirmative, it must also be acknowledged that other instruments could not have been used, or at least that this very instrument – the EHR – was chosen, making it more like a public-administration database than an electronic health record.

4. *Some not-encouraging data on the use of the EHR*

Despite coordination and enhancement efforts made, data on EHR implementation, use and deployment have not always been comforting. As AGID's monitoring has attested over time, all Italian regions have been "active" (in the sense that in every Italian region there has been at least one EHR activated in recent years) and each of them has then implemented the tool, equipping itself with the necessary structures to make the file operational in its own territory. However, data on the actual dissemination of the EHR have not been entirely encouraging.[37]

In general, there has been almost negligible use of the EHR by citizens in most Italian regions: for instance, according to available

cipio di accountability, in *Comparazione e diritto civile*, 2022, 1 ff.; G. Finocchiaro, *Il principio di accountability*, in R. Caterina (ed.), *GDPR tra novità e discontinuità*, in Giur. it., 2019, 2778 ff.

[33] A. Mantelero, *La gestione del rischio*, in G. Finocchiaro (ed.), *La protezione dei dati personali in Italia. Regolamento UE n. 2016/679 e d.lgs. 10 agosto 2018, n. 101*, Bologna, Zanichelli, 2019, 473 ff.; Id., *Il nuovo approccio della valutazione del rischio nella sicurezza dei dati. Valutazione d'impatto e consultazione preventiva (artt. 32-39)*, in G. Finocchiaro (ed.), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, 287 ff. See Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 4 October 2017, WP 248 rev.01.

[34] N. Brutti, *Le figure soggettive delineate dal GDPR: la novità del data protection officer*, in E. Tosi (ed.), *Privacy Digitale. Riservatezza e protezione dei dati personali tra GDPR e nuovo Codice Privacy*, Milano, Giuffrè, 2019, 115 ff.

[35] This is all the more so when one considers the corresponding requirement in Article 6 of the Regulation. See D. Poletti, *sub* art. 6, in R. D'Orazio, G. Finocchiaro, O. Pollicino and G. Resta (eds.), *Codice della privacy e* data protection, 194 ff. Strictly interpreting the parallel criterion of Article 7 of Directive No. 46 of 1995, the Article 29 Working Party, *Opinion 6/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 9 April 2014, WP217. In case law, see ECJ EU, 16 December 2008, Case C-524/06 (*Huber*), in *www.curia.europa.eu.*

[36] «In so far as it provides for an exception to the principle that the processing of special categories of personal data is prohibited, Article 9(2) of the GDPR must be interpreted strictly». ECJ EU, 4 July 2023, Case C-252/21 (Meta Platforms), in www.curia.europa.eu.

[37] N. Posteraro, *La digitalizzazione della sanità in Italia: uno sguardo al Fascicolo Sanitario Elettronico (anche alla luce del Piano Nazionale di Ripresa e Resilienza)*, in *www.federalismi.it. Osservatorio di diritto sanitario*, 17 November 2021.

data,[38] usage thresholds above 50 per cent were reached only in two regions in the second quarter of 2022; and only in one - Emilia-Romagna - in the fourth quarter of 2022.[39]

It is believed that the main reasons for this lack of (or in any case low) use are to be ascribed (if not exclusively, at least also) to the population's insufficient digital skills and to a certain resistance to change in daily habits (which probably depends precisely on the lack of knowledge of the technologies to be used: individuals' confidence in innovation and their ability to adapt to it are, in fact, often linked to the degree of knowledge of digital tools, both in terms of their actual potential and the risks that may arise from their use). This digital incompetence of the population evidently affects the telematic interaction between citizens and public administrations: with regard more specifically to the health sector, as revealed in a research conducted by the Osservatorio Innovazione Digitale in Sanità of the School of Management of the Politecnico di Milano,[40] eight out of ten citizens do not use web-based health services. 86 per cent of patients prefer to seek medical advice in person, 83 per cent go to counters to pay for services, and in 80 per cent of cases they pick up their reports by hand. It is therefore not surprising that, at least on the side of the patients, a tool such as the Electronic Health Record has been struggling to take off.

With regard, on the other hand, to use by licensed physicians, in 2022 there were indeed increasing percentages - compared to those recorded in 2021 - and higher percentages (compared to use by citizens). Thus, for example, it turned out that, in the second and fourth quarters of 2022, physicians in sixteen Regions and Autonomous Provinces used it, reaching percentages above 98% in only six Regions (Emilia-Romagna, Lombardy, Apulia, Sardinia, Aosta Valley, Veneto) and in the Province of Trento. In the fourth quarter of 2022, however, doctors in only two Regions (Umbria and Aosta Valley) fed it with the patient's summary health profile.[41]

On the other hand, the percentages relating to the number of healthcare workers who, out of the total of regional healthcare workers, are enabled to use the EHR, albeit to a relatively modest extent, were increasing compared to those recorded in 2021: according to the data from the fourth quarter of 2022 or referring to the last update surveyed by the individual Regions, only in eight of the Regions and Autonomous Provinces did the percentage exceed 50% (Emilia-Romagna: 66.23%; Lombardy: 100%; Piedmont: 83.65%; Apulia: 80.08; Sardinia: 95.25%; Tuscany: 100%; Veneto: 89%; Trento: 100%); in the others, it stood at decidedly low values (e.g. Abruzzo: 7.5 %; Basilicata: 10%; Campania: 30.71%; Friuli-Venezia Giulia: 23.29%; Marche: 19%; Molise: 3%; Sicily: 20.42%; Aosta Valley: 31%).[42]

It is clear, therefore, that it was from the outset an ambitious and challenging project for the Italian context (characterised, in actual terms, not only by a strong regional fragmentation, but also by a significant delay in digital growth, as the data show).

[38] See *www.fascicolosanitario.gov.it/monitoraggio*. Data are updated quarterly and, when the latest quarterly update is not available, reference is made to the latest available update.

[39] The indicator gives an account of the number of citizens who, out of the total number of patients for whom at least one report has been made available, have made at least one access to their EHR in the last 90 days of the monitored period.

[40] The results of the survey are reported as part of the online conference "Sanità digitale oltre l'emergenza: più connessi per ripartire" on 26 May 2021, organised by the Osservatorio Innovazione Digitale in Sanità of the School of Managment of the Politecnico di Milano (*www.osservatori.net/it/eventi/on-demand/convegni/convegno-risultati-ricerca-osservatorio-innovazione-digitale-sanita-convegno*).

[41] In 2021 the number of physicians and healthcare workers who, compared to the total number of licensed general practitioners and paediatricians of free choice, used the EHR in the exercise of their profession was still very low: according to the data then available, in the second quarter of 2021, only physicians in 9 Regions had used the EHR and in two of them, moreover, very low percentages were recorded (we refer, in particular, to Lazio, which reached the percentage of 22%; to Piedmont, which reached 3%; to Tuscany, which reached 10%. The results of the other 7 Regions were good: Emilia-Romagna: 100%; Friuli-Venezia Giulia: 74%; Lombardy: 100%; Apulia: 99%; Sicily: 99%; Aosta Valley: 100%; Veneto: 99%); furthermore, with respect to the total number of activated EHRs, only the physicians of 3 Regions, in the same period considered, had concretely fed it – however slightly – with the patient's synthetic health profile (and in one of the 3 – Friuli-Venezia Giulia – it had been implemented by only 1% of the physicians).

[42] In the second quarter of 2021, however, the percentage exceeded the 50% threshold in only six regions (Emilia Romagna: 60.62%; Lombardy: 100%; Piedmont: 76.2%; Apulia: 71.6%; Tuscany: 100%; Veneto: 89%); in the others, the thresholds reached were very low, or zero (Calabria: 0%; Campania: 0.74%; Friuli Venezia Giulia: 23.29%; Lazio: 0%; Sicily: 14.42; Aosta Valley: 31%).

The current national panorama was also taken into consideration by the Guidelines approved by the EHR Working Group on 25 January 2022 – to which we will return below – from which it emerged that the conception of the EHR has always appeared rather basic and its implementation characterised by only partial dissemination of services on the territory, incomplete implementation of the minimum core of documents, documental inhomogeneity, limits, shortcomings and systematic shortcomings. Moreover, an uneven feeding of the file was noted, so that, even in the Regions where the minimum core was implemented, the EHR was not then fed in the same way by all healthcare facilities. In any case, the low or incomplete feeding of the file has resulted in its inability to respond to the user's needs regarding his or her care and to provide a valid and reliable care tool for healthcare professionals.

5. *The EHR in the context of the National Recovery and Resilience Plan*

The Italian National Recovery and Resilience Plan (NRRP) highlighted that the COVID-19 pandemic has confirmed the universal value of health and its nature as a fundamental right. In particular, it pointed out that our NHS in general is able to provide adequate health outcomes and a high life expectancy at birth;[43] then, it also stressed that the pandemic has made more evident some structural criticalities of the aforesaid NHS (critical aspects that could be aggravated by the increased demand for care resulting from the demographic, epidemiological and social trends currently underway).[44]

The strategy that the NRRP pursues is therefore aimed precisely at tackling all these critical aspects in a synergetic manner. The Plan specifically devotes Mission 6 to health, allocating a total of 15.63 billion euros to it. The NRRP emphasises how the health emergency has shown, among other things, the importance of being able to count on an adequate use of the most advanced technologies and on high digital skills (as well as professional and managerial skills): the pandemic – it specifies – has highlighted how healthcare is an area that requires significant digital upgrading;[45] consistently, it allocates a large part of the aforesaid resources to improving infrastructural and technological endowments, as well as to developing skills, including digital skills of personnel.

The Plan embraces the potential of the EHR, defining it as a "cornerstone" for the provision of digital-health services and the enhancement of national clinical data:[46] from this perspective, for example, it proves relevant the part of the Plan that states that telemedicine projects proposed by the Regions on the basis of the priorities and guidelines defined by the Ministry of Health may be financed only "where they can be integrated with the electronic health record".

The main objective of the NRRP is to strengthen the EHR, in order to ensure its dissemination, homogeneity and accessibility throughout the country by patients and health workers.

In the light of what has been noted above, the part in which the Plan expressly alludes to the need to invest in (in order to improve) the digital skills of the population[47] certainly appears important; the project is destined to really take off only with the effective participation of all the stakeholders of the health ecosystem, including, first and foremost, the patients.

However, it is believed that this type of activity, while certainly appreciable, will not be sufficient to ensure the effective dissemination of the tool, given that individuals, even when they are digitally competent, will refrain from using the EHR if they are not made aware beforehand of its potential and actual functioning, with a focus on the processing of the personal data that flow into it: a recent survey conducted in 2021 by the "Osservatorio Innovazione Digitale in

[43] Despite the fact that healthcare expenditure on gross domestic product is lower than the EU average.

[44] See N. Posteraro, *Complexity and complication of the italian healthcare system: can e-health be a possible solution?*, in M. De Donno and F. Di Lascio (eds.), *Public authorities and complexity. An Italian overview*, Napoli, Jovene, 2023, 161 ff.

[45] On the relationship between the pandemic and increased digitisation of the healthcare sector, see the above-mentioned report 'Digital transformation: Shaping the future of European Healthcare', by the Deloitte Centre for Health Solutions, a Deloitte research centre specialising in healthcare issues and practices. 65% of European respondents say their organisation has increased the use of digital technologies to support the work of healthcare workers following the COVID-19 emergency; a similar percentage (66%) for Italy.

[46] See p. 17 of the Plan, which also refers to the EHR in sections other than the one strictly devoted to the Health Mission.

[47] P. 86 ff. of the Plan.

Sanità" of the Politecnico of Milan[48] shows that Italians have not a good perception of what the Electronic Health Record is and how it works. It turns out, in fact, that only 38% of the population has heard of it and only 12% is aware of having used it.[49] This would explain the mismatch, noted above, between the number of active records and the percentage of actual use of the tool (consultation and access). As things stand, adequate awareness-raising campaigns on the use of the EHR must therefore be promoted.

Equally appreciable, then, is the part in which the NRRP alludes to investment in the digital skills of medical-health personnel: investing in the training of citizens, in fact, is not enough; it is also necessary to work on the training of socio-healthcare personnel, who must actually use the tool in their work, if we consider that, at present, as highlighted earlier, the number of doctors and health-care workers who use it in their profession is still very low.

Significant from this point of view are the data from the survey – referred to above – of the "Osservatorio Innovazione Digitale in Sanità". They evidence that although 60% of specialist doctors and general practitioners have sufficient basic digital skills, mostly linked to the use of digital tools in daily life, only 4% have, to a satisfactory degree, the digital skills necessary for the medical-health profession. With regard to the digital skills of younger doctors, the findings of the survey conducted in February 2020 by the scientific task force of the *Validate*[50] project are equally relevant. The online survey – which involved a sample of 362 doctors under the age of 35 – found that only 13% of them had experience with *Big Data*, predictive models and artificial intelligence; while only 6% had experience with the *Internet of things*.

When investing in the digital skills of healthcare professionals, special attention must also be paid to the unavoidable issue of personal-data processing. This is also with a view to preventing damage resulting from data breaches in the healthcare sector: the ongoing sanctioning activity of the Italian Data Protection Authority is proof of this. In this regard, it is worth recalling the measures of 2 July and 9 July 2020, with which the Authority admonished two healthcare facilities for security breaches, albeit limited, resulting in the unlawful processing of healthcare data.[51] In the first case, a person who had requested a paper copy of his own medical record was mistakenly given that of another patient; in the second case, a patient found in his electronic health record a report on a different person. Both episodes denote the need not only to encourage the preparation of appropriate organisational measures to ensure the security of processing, but also to raise the awareness of the staff who are actually required to process such data.

6. *The EHR implementation Guidelines. Evolving perspectives*

In order to ensure that the objectives that the EU requires for the disbursement of funds are achieved within the timeframe set out in the NRRP, the EHR Implementation Guidelines were drawn up. Adopted by Decree of the Ministry of Health of 20 May 2022 and published in July of the same year, they are intended to summarise and amend all previous recommendations and become the basis for implementation up to 2026.[52]

The EHR must become – they say – the

[48] The results of the survey are reported as part of the above-mentioned online conference "Sanità digitale oltre l'emergenza: più connessi per ripartire" on 26 May 2021, organised by the "Osservatorio Innovazione Digitale in Sanità" of the School of Managment of the Politecnico di Milano.

[49] The problem of patients' lack of knowledge of the tool has already been highlighted by G. Comandè, L. Nocco and V. Peigné, *Il fascicolo sanitario elettronico: uno studio multidisciplinare*, in *Rivista italiana di medicina legale*, 2012, 105 ff. More than ten years later it does not appear that things have actually changed.

[50] The national survey was conducted in cooperation with the Associazione Segretariato Italiano Giovani Medici (SIGM) and the Istituto Superiore di Sanità. The Validate project (Value-bAsed Learning for Innovation, Digital-health, Artificial inTelligencE) aims at the definition, structuring and dissemination of specific skills and competences in the field of e-Health with particular reference to young doctors.

[51] These are decisions No. 123 and No. 141 of 2020. See decision No. 371 of 10 November 2022, in which the GPDP imposed a fine of EUR 40,000 on a healthcare facility for breach of the GDPR rules, with reference to the processing of personal data carried out by means of a health record. Without claiming to be exhaustive, see also decisions No. 27, 29, 30 and 36 of 27 January 2021, No. 45 of 11 February 2021, No. 142, 144 and 145 of 15 April 2021, No. 211 and 212 of 27 May 2021, No. 34 of 27 January 2022, and No. 200 and 201 of 26 May 2022.

[52] These Guidelines were issued pursuant to Article 12(15-*bis*) of d.l. No. 179 of 2012, as amended by d.l. No. 4 of 2022, precisely in order to enhance the EHR. S. Corso, *Le Linee guida di attuazione del fascicolo sanitario elettronico*, in *www.rivistaresponsabilitamedica.it*, 31 July 2022. The text of the Guidelines is available at *www.agid.gov.it*.

single and exclusive point of access for citizens to national health-system services. It will be an ecosystem of data-based services for healthcare professionals for the diagnosis and treatment of their patients and for increasingly personalised patient care, as well as a tool for healthcare facilities and institutions, which will be able to use the clinical information in the EHR to perform clinical-data analysis and improve healthcare-service delivery.

There are four actions envisaged by the Guidelines to strengthen the EHR: 1) guarantee homogeneous and uniform digital-health services; 2) standardise contents in terms of data and coding; 3) improve interoperability of the EHR; 4) strengthen the governance for implementing the new EHR.

For each action – i.e. services, content, architecture and governance – the Guidelines define EHR requirements and recommendations – for the the short, medium and long term – necessary to achieve the objectives set by the NRRP.

It is not possible here to review all the requirements listed in the guidelines, but it may be useful to mention some of them.

The mandatory requirements to be implemented in the short term include, as regards the standardisation of access services, managing consents to consult documents in the file, withholding specific clinical documents or types of clinical documents, and managing proxies.

Among the mandatory requirements, in addition to the evolution towards services for accessing clinical data – not only just documents – are the innovation of the EHR architecture, complete with a central clinical-data repository,[53] and the adoption of Advanced Analytics tools, also based on artificial-intelligence techniques for processing clinical data in the EHR.

Added to this, in terms of services, is access to telemedicine, for the provision of "tele-visits" by doctors, tele-assistance and tele-consultation.[54]

For health institutions, the EHR represents the knowledge base on the health status of the Italian population, at all levels of the NHS, for the definition and implementation of prevention and health-planning policies. Therefore, it will provide services – it says – to support the decisions of policy makers and the clustering of patients in relation to their respective clinical and health conditions.

Among the recommended requirements, on the other hand, is the provision to healthcare institutions, for governance purposes, of data, i.e. the knowledge base useful for governing regional and national public health policies, also through the implementation of value-based care strategies, i.e. the effectiveness and actual benefit generated on the patient by the healthcare services provided. In this context, the EHR will implement: data extraction, pseudo-anonymisation and preparatory functions that healthcare institutions can use to: organise and modulate healthcare around individual pathologies and groups of patients with similar needs; measure outcomes and costs for each patient, i.e. consistently measure value, understood as the relationship between health status and the costs of the care cycle; adopt value-based reimbursement models.

The Guidelines then illustrate the benefits for the citizen, both direct, in relation to treatment, and indirect, through the advantages enjoyed by the public administration. These include those deriving from research, which will be able to make use of EHR data, for which its enrichment with omics, genetic and epigenetic data is recommended.

The EHR will become the main information and health-education tool, with the aim of promoting health awareness among citizens. In this sense, the EHR will also realise patient empowerment in care.

The National Agency for Regional Healthcare Services (AGENAS), which is expressly recognised as the National Digital Health Agency,[55] will also contribute to achieve the objectives of the NRRP.

The legislative and technological development of the EHR will, in any case, have to reckon with the new rules of European-Union law. The reference here is to the proposal for a Regulation of the European Parliament and of the Council on the European health data space (COM(2022) 197 final), presented by the European Commission. Indeed, on 3 May 2022, the Commission launched the European Health Data Space (EHDS). This space, as stated in

[53] And it will already be completed with the Health Data Ecosystem (EDS).

[54] R. Senigaglia, *Telemedicina ed essenza fiduciaria del rapporto di cura, in Persona e mercato*, 2023, 470 ff.

[55] Article 12(15*decies*) d.l. No. 179 of 2012.

the relevant press release, will enable people to control and use their health data both in their own country and in other Member States, promote a single market for digital health services and products, and provide a coherent, reliable and efficient framework for the use of such data in research, innovation, policy-making and regulation, while respecting the Union's high standards of data protection. This is the first Common European Data Area in a specific field and is part of the European Data Strategy.[56]

It is just worth mentioning that, at the European level, a decisive impetus for data-related innovation has already been given by EU Regulation No. 868 of 2022 (Data Governance Act), especially through the regulation of data re-use and altruism. Further impetus towards enhanced data-based services will be provided by the new EU Regulation No. 2854 of 2023, on harmonised rules on fair access to and use of data (Data Act).

The introduction of these new systems - and sub-systems - of rules at the supranational level, in the area of data processing, as well as their impact on the regulation of health data, may also affect cross-border healthcare.[57]

Certainly, in the multiplication of regulatory references, the intersecting levels of sources, and the overlapping of regulated topics, one of the greatest challenges for the legislator will be to coordinate the various provisions and compose a legal framework that can guarantee certainty.

7. *The detailed discipline: the decree published in 2023*

The detailed discipline of the EHR was first laid down in the "Regulation on the electronic health record", set out in Prime Ministerial Decree No 178 of 29 September 2015, and then in the Ministry of Health Decree of 7 September 2023, entitled "Electronic Health Record 2.0" ("EHR 2.0 decree").

Published in the Official Gazette on 24 October 2023, the EHR 2.0 decree intervenes on the legal-reference framework, updating the provisions to the technological and regulatory evolution of the electronic health record.

Issued pursuant to Article 12(7), of d.l. No. 179 of 2012, it is the result of a long institutional interlocution and of multiple adjustments, as evidenced by the provisions of the Italian Data Protection Authority No. 294 of 22 August 2022 - which expressed a non-favourable opinion on the draft decree of the Ministry of Health[58] - and No. 256 of 8 June 2023, which expressed a positive opinion in relation to the draft decree on the HER.[59]

Therefore, the Prime Ministerial Decree No. 178 of 2015 ceased to be effective as of 24 October 2023 except for the provisions of Chapters III and IV,[60] which remain in force until the adoption of the further decrees[61] for the provisions on the processing "of data and

[56] S. Corso, *Lo spazio europeo dei dati sanitari: la Commissione Europea presenta la proposta di regolamento*, in *www.federalismi.it. Osservatorio di diritto sanitario*, 10 August 2022; Id., *European Health Data Space. La Commissione europea presenta la proposta di Regolamento sullo spazio europeo dei dati sanitari*, in *www.rivistaresposabilitamedica.it*, 13 June 2022; Id., *Una strategia europea per i dati, anche sanitari*, ivi, 7 March 2021. See European Commission press release, European Health Union: A European Health Data Space for people and science, 3 May 2022, in www.ec.europa.eu. On this proposal for a regulation, the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS) adopted a joint opinion on 12 July 2022. S. Corso, Il parere congiunto del Comitato europeo per la protezione dei dati e del Garante europeo della protezione dei dati in merito alla proposta di Regolamento sullo spazio europeo dei dati sanitari, in www.rivistaresponsabilitamedica.it, 5 September 2022.

[57] See N. Posteraro, *Cure oltre lo Stato: l'effettività del diritto alla salute alla luce del d.lgs. n. 38 del 2014*, in *www.federalismi.it*, 23 November 2016; Id., *Active international healthcare mobility and urban accessibility: the essential role of Italian cities and urban planning in the development of foreign healthcare tourism*, ivi, 13 January 2021. See European Commission Recommendation 2008/594/EC of 2 July 2008 on cross-border interoperability of electronic health record systems, and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on telemedicine for the benefit of patients, healthcare systems and society, COM(2008) 689 final, 4 November 2008. For particular relevance, also of a comparative nature, see the studies by F. Lupiáñez-Villanueva et al., *Study on Health Data, Digital Health and Artificial Intelligence in Healthcare*, Luxembourg, Publications Office of the European Union, 2022, and J. Hansen et al., *Assessment of the EU Member States' rules on health data in the light of GDPR.*

[58] S. Corso, *Fascicolo sanitario elettronico ed ecosistema dati sanitari. I pareri critici del Garante per la protezione dei dati personali al Ministero della salute*, in *www.rivistaresponsabilitamedica.it*, 22 september 2022.

[59] N. Posteraro, *Parere del Garante privacy sullo schema di decreto sul Fascicolo Sanitario Elettronico (FSE)*, in *www.federalismi.it, Osservatorio di diritto sanitario*, october 2023.

[60] Article 27(5), of the EHR 2.0 decree.

[61] To be issued in implementation of Article 12(7) of d.l. No. 179/2012.

documents" of the EHR for research and government purposes.[62] Thus, Articles 15-17 and Articles 18-20 of Prime Ministerial Decree No. 178/2015 are still applicable for processing for research purposes and processing for government purposes, respectively.

The EHR 2.0 decree, as announced in Article 2, identifies the contents of the EHR, the limits of the responsibilities and tasks of the parties involved in its implementation, the guarantees and security measures to be adopted in the processing of personal data with respect to the rights of the assisted person, and the modalities and different levels of access to the EHR.

The decree only partially innovates the previous discipline, maintaining in many aspects the same choices made previously.

Undoubtedly positive is the attention shown by the new provisions with regard to the identification of the data controller of the data processed by means of the EHR, since the EHR is established at the Regions and Autonomous Provinces, but may be used, for different purposes, by several entities on the basis of different legal requirements.

An important new feature of the EHR 2.0 decree is to provide liability for the persons responsible for feeding the EHR for failure to do so, or for untimely or inaccurate feeding.[63] The disposition treasures the indications expressed by the Italian Data Protection Authority, in provision No. 294 of 2022, which highlighted, as a critical point of the discipline, the absence of a real obligation to upload data and documents in the EHR, given the lack of a rule expressly providing for a liability for specific subjects.

The operations executed on the EHR are recorded. The patient can view the recordings made[64] and he is notified of the operations carried out on hir or her HER.[65]

Similarly to the previous 2015 regulation, the 2023 decree specifies that consultation of EHR data and documents, for purposes of diagnosis, treatment and rehabilitation, prevention, international prophylaxis - not for purposes of study and scientific research or health governance - is subject to the prior consent of the patient, pursuant to Article 8 of the EHR 2.0 decree, which reproduces the requirements enshrined in the GDPR: consent must be freely given, specific, informed and unambiguous as well as granular, i.e. expressed for each purpose of processing, and - for sensitive data – explicit.[66]

Another relevant issue of the EHR 2.0 decree is the actual possibility for patients to delegate other parties to access their EHR and the power to express consent to consultation.[67]

With regard to emergency access, a rule is now laid down that respects the confidentiality and self-determination of the patient. The case regulated is that of a person who has not given consent to consult the EHR, who is in a condition of physical impossibility, incapacity to act or natural incapacity, and at the same time is at serious, imminent and irreparable risk to his or her health or physical safety. In this case, health professionals and practitioners may first access the patient's summary and, only where necessary, once the inability to give consent has been verified, also the other data and documents in the EHR, limited to the time needed to provide treatment and except for those that he or she has decided to obscure.[68]

8. *The content of the EHR*

The EHR is an instrument subject to continuous feeding over time, rich in heterogeneous data and documents. In the light of the 2015 internal provisions,[69] it had to include a minimum core of elements,[70] but it also could be composed by some others integrative elements, foreseen by the individual Region/Autonomous Province.

Among the necessary elements, the patient summary and the pharmaceutical dossier were particularly important.

The pharmaceutical dossier is a section updated by the pharmacy; it makes it possible to trace (and, if necessary, to reconstruct) the patient's pharmacological history, as well as

[62] Order No 256 of 2023 emphasises the need for the revision of the rules on the processing of personal data through the EHR to be completed as soon as possible, also innovating the rules on the pursuit of health government and research purposes.
[63] Article 12(3), of the EHR 2.0 decree.
[64] Article 21 of the EHR 2.0 decree.
[65] Article 22 of the EHR 2.0 decree.
[66] European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, adopted on 4 May 2020, in www.edpb.europa.eu.
[67] Article 8(5) and 11(8-12) of the EHR 2.0 decree.
[68] Article 20 of the EHR 2.0 decree.
[69] Article 2(2), of the 2015 regulation.
[70] In detail, the EHR must contain the patients' identification and their administrative data, reports, first aid reports, discharge letters, and consent to organ donation.

to monitor the appropriateness of the dispensing of medicines and the fitness to treatment[71] (which can ensure that the use of medicines is optimised and can produce documented results in terms of improving the population's state of health and savings for the NHS[72]). This section has not been adequately developed, in all these years[73] and the new decree published in 2023 expunged it: the dossier will be regulated by the implementing decree of the provisions referred to in paragraph 15-quater of art. 12 d.l. n. 179/2012, as a service rendered available from EDS.

The patient summary, instead, is regulated by the EHR 2.0. decree[74] and can be qualified as a summary of the patient's medical profile drawn up by the so-called "family doctor" (or free-choice paediatrician): it is a document that provides an important support, especially in emergency situations, as it allows health professionals to gain a background on an unknown patient during a sudden and unpredictable contact; it is updated upon changes that are considered relevant to the patient's medical history.

Among the constituent elements, the "personal notebook" has a particular importance: it is a specific area in which patients may personally enter data and documents relating to their treatments.[75] This is a particularly-important additional element, which allows and ensures the active participation of the patients in the construction of their own health databases.[76] In this sense, it promotes attitudes of self-management and empowerment, which are certainly in line with the digital evolution of the citizen, made more autonomous by ICT technologies.

From this point of view, the personal notebook (that was an integrative element, during the validity of the 2015 regulation[77]) thus represents an important evolution of the relationship between the health world and the citizen-patient, since it promotes new forms of dialogue and interaction between doctor and patient, and encourages patients to use the EHR, offering them the possibility to "customize" it. In any case, the entry of data depends on the patients' ability to find them, as well as on the willingness/ability to enter them into the system; therefore, one cannot rule out the possibility that a) patients may refrain from entering because they are not fully able to navigate the platform; b) erroneous or misleading data may be entered: then, the healthcare professionals will have to assess with extreme caution the possibility to consider correct and reliable the data and documents entered in the personal notebook. The question then arises as to how useful an entry of this kind really is, given that it is not followed by a control-filtering carried out downstream by subjects previously identified and appointed for this purpose.

9. *On the right to obscure the data automatically inserted into the EHR*

Article 9 of the 2023 new decree establishes that the patient is free to conceal the data automatically included in the file that they do not wish to make visible, not even to those who are authorised to access them; this is the so-called "obscuration", which is carried out in such a way as to ensure that those authorised to access the EHR for the purposes of treatment cannot automatically become aware of the fact that the patient has made this choice and that such data exist (so-called "obscuration of the obscuration").

In this way, it should be averted the danger of an indirect influence of the current legal framework on the choices of those who prefer not to be treated, rather than disclose certain health treatments - concerning, for example, their sexual sphere -. These are reinforced measures, the rationale for which is to be found in the peculiar sensitivity of health data, which are more subject to possible misuse, even for discriminatory purposes. As noted by Italian scholarship, in fact, health data are part of the "hard core of confidentiality" – to which the right to health is linked by "an indissoluble link"[78] – and, therefore, enjoy

[71] Article 12(2-*bis*) of d.l. No. 179/2012.
[72] See Federfarma, *La farmacia italiana 2020/2021*, cit.
[73] This can be concluded reading the opinions recently disseminated by some professionals in the pharmaceutical sector (see, for example, the reflection of F. Schito, secretary general of Assofarm, in an editorial to the association's June 2021 newsletter, *Digitalizzazione, è il momento del Dossier Farmaceutico*, available at *www.assofarm.it*, as well as by what is expressly reported by Federfarma, *La farmacia italiana 2020/2021*, April 2021, in *www.federfarma.it.*
[74] Article 4.
[75] Article 5.
[76] A.M. Gambino, E. Maggio and V. Occorsio, *La riforma del fascicolo sanitario elettronico*, 5.
[77] The new decree establishes that this section of the EHR will be composed also by the data generated by medical devices and/or wearable.
[78] C. Colapietro and F. Laviola, *I trattamenti di dati per-*

special protection compared to ordinary data. For this reason, under the 2023 regulation,[79] the option to obscure EHR data must be expressly mentioned - along with the other components identified by the rule – in the information provided to patients.

Certainly, also through this action, the EHR solicits the empowerment of the patients,[80] who is called upon to take an active attitude in the management of health information concerning him or her.

The internal rules specify that the request for the obscuring of data and documents can be made both before the file is fed and afterwards:[81] therefore patients can request obscuring when they decide to undergo treatment and are made aware of the processing to be carried out and that their data will be transferred directly to the digital archive. From this point of view, the fundamental moment of prior dialogue between the doctor and the patient must therefore be enriched with new moments of information: in particular, the doctor must remind individuals that the service to be performed, if consented to, will entail the automatic inclusion of the data relating to it in the EHR; and he must at the same time remind them that they have the right to request and obtain the obscuring of the aforementioned data even before the treatment is carried out.

Finally, it should be recalled that, pursuant to the 2023 regulation, the health and socio-health data and documents governed by the regulatory provisions for the protection of HIV-positive persons, women undergoing voluntary termination of pregnancy, victims of acts of sexual violence or paedophiles who use drugs, psychotropic substances and alcohol, women who decide to give birth anonymously, as well as data and documents relating to the services offered by family-advice centres, can only be visible with the explicit consent of the interested person:[82] in this case, therefore, the active action of the individual patient, subsequent to the automatic implementation of the data in the EHR, is not aimed at hiding what is otherwise visible, but at making visible what otherwise, *ex lege*, would not be visible.

It must be considered, however, that some information may be missing from the EHR, and the gap may be, if not real, at least virtual, if the patients have exercised their right to obscure the data.[83] The healthcare professional must then be aware that the EHR can always give only a partial view of the patient's medical history.

The possible non-exhaustiveness of the visible and searchable collection of data carried out by means of this instrument therefore also implies its potential incompleteness. The doctor, therefore, cannot afford to rely entirely on the EHR, since it could prove detrimental to the patient, as decisions concerning his or her health could be taken on the basis of a partial and, on the whole, inaccurate compendium of information.[84]

sonali in ambito sanitario, in *www.dirittifondamentali.it*, No. 2, 2019, 6 ff.

[79] Article 7 and article 9(2).

[80] G. Fares, *The processing of personal data concerning health according to the EU Regulation*, in G. Fares (ed.), *The Protection of Personal Data Concerning Health at the European Level. A Comparative Analysis*, 17 ff., especially 19.

[81] Article 9(3).

[82] Article 6.

[83] V. Peigné, Il *fascicolo sanitario elettronico, verso una «trasparenza sanitaria» della persona*, in *Rivista italiana di medicina legale*, 2011, 1535 ff.

[84] S. Corso, *Il fascicolo sanitario elettronico fra e-Health, privacy ed emergenza sanitaria*, 404. The probable incompleteness of the EHR was recently reiterated by the Data Protection Authority in a recent ruling (Decision No. 294 of 2022).

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 201-210
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 15

*Digital Therapeutics: An Ongoing Revolution**

Giulia Caldera
(MedMal Claims and Insurances Junior Specialist)

ABSTRACT This article deals with the much-debated topic of digital therapeutics. Starting from a general overview of the role that technology has carried out in the medical field since first innovations, this paper means to highlight the essential support that technlogy has provided, especially during the Covid-19 pandemic, which has made evident the necessity or, at least, the possibility of rethinking medical science in a more digital perspective. This article is aimed to focus on digital therapeutics, which is a specific type of technological product (such as gadgets and medical devices), highlighting remarkable differences that exist within the nebulous world of digital health, starting from the need for digital therapeutics to be supported by a clinical trial that proves its efficiency.
Moving on to the different types of diseases that can be treated, we can mention some concrete examples of digital therapeutics: Deprexis and ReSet, a cognitive-behavioral therapeutics, and Endeavor, an interactive game. In order to understand the substrate on which digital therapeutics is inserted, it is mandatory to address the issues of global regulation of this kind of therapies. Starting from the US context, in which digital therapeutics was born and authorized for the first time by the Food and Drug Administration, we reach the EU case, in which few countries are open up to this technology: in this regard, we mention the experiences of Italy, Germany, Belgium, France and England. In the end, the article examines the critical issues and potential that digital therapeutics represent for health systems.

1. *Digital Therapeutics: a new frontier for modern medical science*

Medical science has always represented a challenging test bed for technology which, from time to time, brings into play solutions ranging from the improvement of services to the optimization of treatment pathways, from the reduction of the adverse effects of treatments to de-hospitalization. In particular the research for new therapies, aimed at treating pathologies previously considered incurable or at reducing their side effects, is the area where the efforts of pharmaceutical companies have been most concentrated on, which over the decades have revolutionized existing therapies: we can take into consideration the marketing of biological drugs first and then of genetic therapies, i.e. drugs whose therapeutic effect is determined by an active ingredient that is no longer of synthetic but biological origin, made up of recombination of genes.

The introduction of these therapies inevitably has changed the way of doing research in the health sector, opening the door to a whole series of hitherto unexplored possibilities. It is, as a matter of fact, thanks to this that, in recent years, the "technological need" of health systems has grown exponentially, in parallel with new clinical discoveries and above all, lastly, with the need to deal with the Covid-19 pandemic, which has seriously put to the test health services globally: these phenomena have once again highlighted the therapeutic potential of technology, capable of guaranteeing greater safety and continuity of treatments even in complex and uncomfortable contexts. It is thus on this substrate that we have witnessed the development of the first digital therapeutics, concerning which the international debate is very lively and much confusion still prevails.

The Digital Therapeutics Alliance states that "digital therapeutics (DTx) delivers medical interventions directly to patients using evidence-based, clinically-evaluated software to treat, manage and prevent a broad spectrum of diseases and disorders". In other words, it is an application of the so-called Digital Health which is expressed in a real cure delivered through the active role of technology, which is no longer conceived as a mere support for pharmacological therapy, but as the main or single treatment. This statement is already indicative of the revolutionary scope of Digital Therapeutics, whose active principle is not a molecule, as in the case of pharmacological therapies, but an algorithm that structures the treatment that the patient must undergo on the basis of the information provided by the doctor or by the patient

* Article submitted to double-blind peer review.

himself or herself.

If, DTx undoubtedly falls within the great category of Digital Health, as highlighted above, it is however not easy to understand what is meant by this term.

First of all, outside the scope of Dtx are all those devices aimed at simplifying and enabling the very delivery of services,[1] those applications having a patient-information function as well as all AI and robotics applications used at the clinical level.[2]

Likewise, cannot be considered DTx all those technological gadgets (Mobile Health) that are intended to ensure and manage the monitoring of vital parameters, which are supported and screened by clinical trials solely prior to the placing on the market[3] and lacking such characteristics to act in itself as a therapeutic treatment.[4]

Above all, on the other hand, attention must be paid to the distinction between DTx and medical devices, which are the subject of experimentation and clinical validation and are able to measure and intervene on the patient's health, but in a purely auxiliary function. These devices, in fact, are characterized by the support that technology offers in the prevention, management and treatment of the pathology, without it representing an essential element of the cure. This distinction between medical devices and DTx is not so intuitive, as clinical-trial data on the subject show.[5]

Therefore, to summarize the elements that distinguish DTx from other Digital Health applications, the following aspects can be highlighted:

- Digital therapeutic treatment (monotherapy or in combination) based on software as an active principle;
- Validation of the efficacy of the treatment following a clinical trial in 4 phases (preclinical phases of research and discovery; clinical phase with clinical development pilot and subsequent clinical development pivotal; submission; post marketing surveillance phase);
- Authorization from regulatory bodies, such as the Food and Drug Administration (FDA) and the European Medicines Agency (EMA, for the centralized authorization or mutual recognition procedure) or national bodies (e.g., AIFA, BfArM, NICE, etc.);[6]
- Medical prescription and possibility of reimbursement by the health system.

As can be guessed, some of these elements are also common to other Digital Health applications (e.g., Telemedicine prescribing or the authorization process for medical devices): the main difference is that only an application that simultaneously meets all of the above requirements is considered DTx.

2. *Digital Therapeutics scope and examples*

Once analyzed the context in which DTx is inserted, it is now necessary to analyze its perimeter, i.e. to understand which pathologies can concretely be treated through the administration of digital therapies. Indeed, the latter obviously cannot be prescribed either whenever surgery is necessary or for diseases and conditions in which the patient's compliance has a limited role (think of the case of a fracture to the femur or removal of a tumor mass). Otherwise, DTx tends to prefer those pathologies that require long-term therapeutic-assistance pathways for which the administration of a drug can be replaced, hence mainly chronic, psychological or central-nervous system pathologies.

Towards these pathologies, digital therapeutics' approach may be implemented in various ways, starting from the preparation of a cognitive-behavioral therapy which provides for the active involvement of the patient, seeking the implementation of

[1] Think in this regard of apps or digital services for booking services or consulting reports.

[2] This includes Telemedicine (in all its forms: telemonitoring, telehealth, teleconsultation, telerehabilitation, etc.), surgical robots and nanorobotics.

[3] The main difference between clinical trials related to Mobile Health and Digital Therapies is that the latter are also subject to Real World Evidence, i.e., verification of effects and outcomes in medical practice following authorization and marketing.

[4] Examples include smartwatches, smart bracelets, sensors that can detect ingested medications, etc. Thus, these are useful tools for human-health management, yet they are a support and not a therapy.

[5] As reported by Professor Eugenio Santoro during the webinar *Terapie Digitali: dallo sviluppo alla pratica clinica. Una rivoluzione possibile*, held by the Osservatorio Terapie Avanzate on 14 October 2022, many studies on digital therapies were subject to review and exclusion once it was ascertained that they were merely observational studies or experiments relating to mere-support tools. Out of 560 studies considered, as a result of these reviews, only 136 actually resulted in DTx.

[6] Thanks to their nature as a therapeutic treatment, hence, digital therapeutics are subject to a process of research, experimentation and authorization for prescription and marketing similar in terms of timing and regulation to that envisaged for any other drug.

corrective behaviors and/or of one's own situation.

Precisely committed to this purpose is Deprexis, the first digital therapy approved in the world in 2009, created by the Gaia company. Deprexis was developed in Germany for the treatment of what is estimated will be the most common disease in the world by 2030: depression. The basic algorithm of Deprexis is structured in order to provide a 12-week cognitive-behavioral therapy (CBT) as an alternative to the traditional psychological/psychiatric path: the platform is actually able to interact with the patient as a real therapist, analyzing the answers provided with the aim of returning a personalized therapeutic path available 24 hours a day, 7 days a week, on any technological device.

The basic idea of Deprexis was subsequently taken up and developed, among others, by ReSet, authorized by the Food and Drug Administration (FDA) in 2017 as the first DTx in the USA. Marketed by Pear Therapeutics, undisputed leader in the research and development of digital therapeutic area, ReSet was created for the treatment of addictions in the form of an app.[7]

The standard treatment provided for substance dependence (alcohol, smoking, drugs, etc.) takes the form of a multi-professional approach involving different roles (psychologists, psychotherapists, psychiatrists, educators, social workers, etc.) and includes rehabilitation programs in dedicated structures or structured with the aid of therapies, whether pharmacological or rehabilitative. On the other hand, through the insertion of data (e.g. those relating to craving, i.e. the impulse to take substances) that influence its algorithm, ReSet returns a cognitive behavioral therapy lasting 12 weeks, with a recommended dosage of 4 "doses" per week. The digital treatment the patient[8] accesses is represented by interactive lessons, feedback, advice, corrective exercise of their habits modules which are designed precisely on the basis of the information provided by the patient, who also always has the possibility of requesting medical assistance. Furthermore, not only might ReSet be prescribed for the outpatient treatment of addicted patients, but it is also constantly subject to the supervision and monitoring of a clinical professional, who also has the possibility of repeating the treatment prescription, whenever necessary to continue for a period longer than 12 weeks. The structuring of the treatment proposed by ReSet makes it suitable for use as a standalone (monotherapy) or plug-in treatment, i.e., as a support and enhancement to the pharmacological / psychological treatment.[9]

Conversely, Akili Laboratories adopted a total different approach beyond the creation of Endeavor, DTx authorized in 2020 by the FDA for the treatment of children between 8 and 12 years of age suffering from Attention Deficit Disorder with Hyperactivity (for short "ADHD").[10] Endeavor has entered this context using the Akili Selective Stimulus Management Engine (SSMETM)[11] technology, designing an interactive-action videogame customized according to the

[7] A later version, ReSet-O, is specifically aimed at the treatment of opiate addiction.

[8] At present, ReSet is only prescribable to patients over 18 years of age.

[9] The potential of ReSet was immediately evident and also confirmed by studies, such as the randomized one carried out on 507 patients for a duration of 12 weeks, in which people were divided into 2 groups according to whether they used the "classic" treatment or ReSet[9]: the study returned the photograph of a strengthened compliance of the patients to whom ReSet had been prescribed compared to those who had benefited from a face-to-face psychological treatment path. This positive outcome can be traced back to various factors, among which undoubtedly stands out the major responsibility of the patient, who is directly involved as a partner in the treatment and not as a passive subject, and the possibility of using this treatment in any place and at any time, ensuring greater privacy compared to the social stigma that often characterizes addiction treatment. To learn more about this, see A. Biondino, *Arriva ReSet, l'app per curare le dipendenze*, in *Nurse Times*, August 2018 (*https://nursetimes.org/arriva-reset-lapp-per-curare-le-dipendenze/54670*), and *Se il medico prescrive un digiceutico*, in *About Pharma*, January 2019, via *www.aboutpharma.com/blog/2019/01/30/se-il-medico-prescrive-un-digiceutico/*

[10] The symptoms of ADHD are mainly inattention, impulsivity and easy distractibility, thus affected children and adolescents show greater difficulty in maintaining concentration and completing assigned tasks; for these reasons, although there are different approaches in the USA and Europe, the recommended treatments for this disorder range from pharmacological therapy to behavioral therapy.

[11] R. Ascione, M. Beccaria, S. Grigolo, G. Gussoni, N. Martini, E. Santoro, A. Ravizza, G. Recchia and V. Rosso, *Digital Therapeutics dalla A alla Z – Storie di Digital Therapeutics - Endeavor*, in *Pharmastar*, July 2020: SSMETM is "a proprietary technology designed for the targeted activation of specific neural systems in the brain for the treatment of diseases with associated cognitive dysfunction" and, therefore, "features specific sensory stimuli and simultaneous motor challenges designed to target and activate the neural systems that play a role key in the function of attention".

characteristics and needs of the individual patient, who must maintain the necessary concentration to achieve objectives and avoid obstacles in order to pass one level after another.[12] This particular element of innovation represents the better effectiveness compared to the classic-educational video games in the treatment of this disorder.[13]

In other words, Endeavor falls within the category of so-called "serious games" and its digital treatment is based on the principle of "gamification"[14] i.e. the administration of an engaged interactive video game which is not perceived by the patient as an imposition or a treatment. Nonetheless, it allows the pursuit of health objectives guaranteeing the involvement and even the enjoyment of the patient.

Among the 36 DTx that have been authorized in September 2022 globally,[15] with a clear predominance of the USA in this sense, Endeavor represents one of the few interactive video-game experiences. On the other hand, the cognitive-behavioral therapies structured in the form of apps in the light of ReSet are more consistent, since they come out more easily suitable to various pathologies (depression, hypertension, diabetes, sleep disorders and insomnia, anxiety disorder, obesity, smoking addiction, etc.).

3. *American and English regulation of Digital Therapeutics*

The undisputed innovative scope of digital therapeutics is indeed the most interesting aspect of these technologies, but also one of the reasons of greatest difficulty for national legislators. As a matter of fact, considering the position taken by individual States in terms of DTx, we are witnessing a real regulatory patchwork.

As far as concerned, it is certainly not surprising that the USA, pioneer in terms of technology, is also the most open country to digital-therapeutic regulation. Since the trade authorization of ReSet in 2017, the FDA has in fact gradually taken on an increasingly proactive approach towards the issue and, with its Digital Health Software Precertification Program[16], has prepared a scheme of approval of the DTx, describing which requirements the interested companies must demonstrate to possess (e.g. an advanced level of security in the management of personal data, a robust quality management system, etc.) and the phases of the approval procedure.

The Digital Health Software Precertification Program, launched in a pilot version in 2017 and completed in September 2022, is joined by the Federal Health IT Program for 2020-2025, which provides the development of a plan for the use of scientifically-validated Digital Therapeutics for the prevention, treatment and management of various pathologies.

The real problem that the USA is facing in relation to DTx is its reimbursement, which, in the absence of a universal or mutual-health system, is left to the discretion of the system. In principle, access to these treatments is actually subject to payment from the user. However, in parallel with the increase in clinical-scientific evidence relating to the effectiveness and efficiency of DTx, there are more and more initiatives by insurance companies aimed at including digital solutions within their portfolios to reduce the hospitalization rate (and re-hospitalization) and the risk profile of their customers. In addition, several companies have also begun to offer digital therapeutics to their employees as a form of corporate welfare. Therefore, it can reasonably be said that this trend will continue to grow in the coming years.

Simultaneously, it is also noteworthy the experience of United Kingdom, whose National Institute for Health and Care Excellence (NICE), in 2018, published some

[12] Game performances - which should include 25-minute sessions to be repeated/5 times a week for at least 4 weeks according to instructions - are recorded by the system and used to return a as-customized-as-possible experience.

[13] As demonstrated by the various studies used for the release of the authorization by the Food and Drug Administration and subsequently published. To deepen, see also S.H. Kollins, D.J. DeLoss, E. Canadas *et al*, *A novel digital intervention for actively reducing severity of paediatric ADHD (STARS-ADHD): a randomised trial*, in *Lancet Digital Health*, 2020.

[14] G. Riboli and V. Alfieri, *L'utilizzo dei videogiochi per una terapia più efficace del Disturbo da Deficit di Attenzione e Iperattività (ADHD)*, in *Lo psicologo del futuro*, n. 12, July 2021.

[15] Source R. Mazzaracca and E. Santoro, *Terapie digitali approvate: a che punto siamo e quali sono?*, in *Advanced Therapy Observatory*, March 2022 (*www.osservatorioterapieavanzate.it/innovazioni-tecnologiche/terapie-digitali/terapie-digitali-approvate-a-che-punto-siamo-e-quali-sono*).

[16] P. Taylor, *Better Therapeutics files for FDA approval of diabetes DTx*, in *Pharmaphorum – bringing healthcare together*, September 2022.

guidelines[17] aimed at ensuring that digital therapeutics be clinically validated, effective, and able to offer economic benefit. These guidelines, revised in 2021, intend to identify the most appropriate levels of evidence depending on the device required by NICE; it should be pointed out, however, that any NICE approval does not automatically allow for reimbursement by the English healthcare system, although it undoubtedly gives support in this regard. To date, the applications Deprexis (for the treatment of depression) and Sleepio (for insomnia[18]) are the two DTx that have obtained NICE approval and reimbursement from the National Health System (NHS).

4. *The regulation of Digital Therapies at the Italian and European levels*

Meanwhile, the situation in the Old Continent is more complex, the regulatory framework is traced by EU Regulation 2017/745 of 5 April 2017 concerning medical devices, which repeals and replaces directives 90/385/EC[19] and 93/42/EC.[20]

This regulation aims to ensure the proper functioning of the internal market for medical devices and a high level of safety of the same and protection of patients' health;[21] analyzing the regulatory text, it can be seen that the European legislator intended to regulate in a single text the regulatory procedures, functional to the evaluation and reimbursement, regardless of whether they relate to medical devices or digital therapeutics.

Indeed, the Regulation apparently brings software used as therapeutic treatment - that is, precisely, digital therapeutics - back within the definition of medical device, which is mentioned both in Article 2[22] as well as in Recital n. 19.[23] This leads one to believe that the heading of the Regulation should be understood in an atechnical sense, whereby it regulates medical devices and digital therapeutics, without dwelling on the intrinsic differences existing between these two categories of technological-health applications, as previously analyzed. In addition, it is pointed out that Article 1 (VI) of Eu Regulation 2017/745 does not expressly include digital therapies within those devices, medicines and materials to which the regulations therein cannot be deemed applicable.

After all, it is the Regulation itself, in Recital No. 8, that provides for the possibility of borderline or otherwise doubtful cases, stipulating that it is up to the Member States to decide on a case-by-case basis whether such devices are subject to the discipline provided therein.

This impression is also confirmed by MDGC 2019/11 (Guidance on Qualification and Classification of Software in Regulation EU 2017/745 - MDR[24]), guidelines prepared by the European Commission for the correct application, precisely, of the Medical Device Regulation (MDR) at the European level. Indeed, while it is true that the Regulation includes software within medical devices, at the same time it does not seem to expressly

[17] This is the Evidence Standards Framework for DHTs, easily reachable on *www.nice.org.uk/about/what-we-do/our-programmes/evidence-standards-framework-for-digital-health-technologies*.

[18] Based on more than a dozen randomized trials submitted to NICE, Sleepio has not only been found to be a viable clinical alternative to classical pharmacological treatment against insomnia, but has also been shown to reduce the direct and indirect costs caused by this condition on the health-care system. This lower economic impact is due to the cognitive behavioral therapy provided by Sleepio as an alternative to pharmacological treatment, which involves recurrent expenses for the purchase of medications and follow-up visits. On the point, R. Mazzaracca, *Trattare l'insonnia con un'app: in UK è realtà*, in *Osservatorio Terapie Avanzate*, giugno 2022, e R. Ascione, *Digital Therapeutics dalla A alla Z - Un mondo a velocità diverse*, in *Pharmastar*, July 2020.

[19] Council Directive 90/385/EEC of 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices.

[20] Council Directive 93/42/EEC of 14 June 1993, on medical devices.

[21] As reported by Recital n. 2 of the EU Regulation 2017/45, "both objectives are being pursued simultaneously and are inseparably linked whilst one not being secondary to the other".

[22] Art. 2 of the EU Regulation defines medical device as "any instrument, apparatus, appliance, software, implant, reagent, material or other article intended by the manufacturer to be used, alone or in combination" for the various medical destinations specified.

[23] Recital n. 19 of the EU Regulation explains that "It is necessary to clarify that software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, qualifies as a medical device, while software for general purposes, even when used in a healthcare setting, or software intended for life-style and well-being purposes is not a medical device. The qualification of software, either as a device or an accessory, is independent of the software's location or the type of interconnection between the software and a device".

[24] In fact, these guidelines also cover EU Regulation 2017/746 on in vitro medical devices.

contemplate the possibility that any therapeutic effect derives from them. In other words, the inclusion of digital therapies within the discipline of medical devices derives from a broadly-oriented interpretation of the term "software".[25]

This inherent ambiguity explains the different speeds and propensities with which Member States have read to concretely apply the Regulation, which entered into force at the European level on 25 May 2017.

4.1. *The Italian experience*

As far as Italy is concerned, for example, the transposition of EU Regulation 2017/745 was supposed to take place within the three-year period following its entry into force, but the Covid-19 pandemic postponed that time by an additional year, making it de facto fully applicable only from May 26, 2021. The problem that was immediately noted, however, lies precisely in the apparent ambiguity of the text, which does not expressly mention Digital Therapies: hence the uncertainty of the domestic legislature in assigning responsibilities to the Ministry of Health or to the Italian Medicines Agency (AIFA). In fact, if, as the Regulations let it be understood, Digital Therapies are to be regulated in the same way as medical devices, they would fall under the competence of the Ministry of Health (Department of Drugs and Medical Devices); on the contrary, were Digital Therapies to be considered drug-therapies, the competence should be avocated to the AIFA as the country's public regulatory body able to authorize them. Until June 2023, no internal legislation had resolved the doubts on the matter, which are reflected in the clinical validation and reimbursability modalities; nonetheless, the legislative proposal submitted on June 7, 2023 to the Chamber of Deputies, specifically titled "Provisions on Digital Therapies," clearly states that DTx is classified as medical devices, in line with European regulations.

Moreover, the aforementioned legislative proposal -currently under consideration by Parliament -represents the first real evidence of awareness of the importance of digital therapies not only for progress but for the very survival of the Italian health care system as well, which has been severely undermined by the repercussions of the Covid-19 pandemic. Structured in 4 articles, the legislative proposal analyzes the possible repercussions that would result from the introduction of DTx in the Italian system: in this regard the law proposes the establishment of an evaluation committee in charge of ensuring a fast track for inclusion in the essential levels of care (so called "LEA"), flanked by a permanent observatory deputed to monitoring and updating the scientific and technological developments of these therapies.[26]

Awaiting regulatory intervention, despite the strong push for technological innovation registered in the last two years due to the pandemic, the diffusion of digital therapeutics in Italy is literally paralyzed: to date, in fact, no DTx has ever been authorized for trade and prescription in the country. In this regard it should be considered that, since Regulation 2017/745 includes software among medical devices and several DTx are already authorized in other member states, a certification to that effect from the Ministry of Health or the Italian Drug Agency would be sufficient for their marketing and reimbursability.[27]

In early 2023, however, the Ministry of Health authorized the start of the Demetra clinical trial, which aims to evaluate weight loss in patients using the new DTxO, involving two Italian health institutions (Istituto Auxologico Italiano and Policlinico Giovanni Paolo XXIII in Bari). "DTxO" is in fact an app designed to treat patients with obesity on an outpatient basis. With a nonpharmacological approach, DTxO provides digital treatment on two levels: on the one hand, it offers dietary plan and patient education/support (dietary and exercise advice program, cognitive-behavioral assessment program, alerts and warnings, chat and televisite); on the other hand, to ensure good patient retention, it is structured in the gamification mode. Hopefully, therefore, Italy

[25] The uncertainty that characterizes the Regulation on the point also makes complex and dangerous the correct risk classification of digital therapies within the categories of medical devices provided and differentiated according to their impact on human health and, therefore, risk. See *Digital therapies, an opportunity for Italy*, in *Tendenze Nuove*, L. Da Ros, G. Recchia, G. Gussoni et al, January 2021, pp. 17-27.

[26] See www.camera.it for the legislative proposal.

[27] It is due to the fact that the verification about the safety and efficacy of these products would already be carried out. On this point also C. Buonamico, *Digital Health and Digital Therapeutics: where are we?,* in *Policy and Procurement in Healthcare*, August 2022.

will also see the first marketing of a digital therapy in the medium term.[28]

In the same vein is the "Digital therapeutics for Obesity", a 2019 project coordinated by the University of Verona and the company DaVinci Digital Therapeutics having as its object the development - by means of a pilot study - of a digital therapy for the treatment of obesity, which is estimated to affect one in ten people in the country. The project, which is still in progress, involves the creation of software capable of monitoring parameters entered by the patient and/or recorded by wearable devices and returning activities to be performed and feedback from the multidisciplinary health team deputed to the patient's care.

Additionally, then, there are notable initiatives, aimed at raising stakeholder awareness of the importance of digital therapies for medicine in line with the clinical, organizational and economic needs of the moment.

Among these, there is the Smith Kline Foundation's "Digital Therapies for Italy" project, which from July 2019 to December 2020 has involved a panel of experts in order to deepen the necessary requirements for the introduction of digital therapeutics in the country. The working group - which has grown over time from the original 21 members to more than 40, representing different technical expertise functional to a fruitful debate - has produced a document[29] that analyzes both the stages of digital-therapeutic development and the stages of introduction into care pathways. Thus different aspects have been examined: the research and development models, the level and nature of evidence of efficacy and tolerability of a digital therapeutic; the terms and criteria for evaluation by regulatory entities as well as for reimbursability; the modalities for the integration of such therapies in medical practice; finally, the conditions to allow Italy to be a user country, but more importantly to join the roster of research countries.

Finally, it must be considered remarkable Vita Acceleratorm, a three-year funding program, which in 2022 selected 6 start-ups engaged in the Digital-Health field – among 120 applications - in order to support the development of both Digital-Medicine and Digital-Therapeutic solutions. Among the start-ups that will benefit from the €6.35 billion fund made available by Vita Accelerator is Sifi, an Italian pharmaceutical company committed to the study of eye diseases and now interested in the creation of a digital therapy for the treatment and maintenance of vision.

4.2. *The European context*

Conversely of a different tenor is the experience of Germany, which is undoubtedly the most active European country in DTx. The turning point came in 2019, when, in the wake of EU Regulation 2017/745, the Bundersat officially adopted the Digitale Versorgung Gesetz (DVG) approved by the Bundestag. Indeed, the DVG paved the way for clinicians to prescribe - often electronically - Digital Therapeutics and specifically medical apps by regulating their reimbursability by private-insurance companies, which are the payers of the German mutual system. To facilitate manufacturers and incentivize them to invest in digital innovation, the German Federal Institute for Medical Devices (BfArM) has devised a pathway structured as follows:

- BfArM approval following clinical-functional validation of digital therapeutics (or DiGA, as it is called in Germany) from the perspective of safety, data protection, functionality and quality;
- Temporary reimbursability for the next 12 months;
- New validation by the BfArM for which manufacturers must demonstrate the app's improved impact on patients' health. Whenever such proof is achieved, the app becomes officially and permanently reimbursable by the health-care system; otherwise, the application for reimbursability cannot be resubmitted.

The fast-track described above is not applicable to any type of DTx, but only for the less hazardous devices, falling in classes I and

[28] The Demetra clinical trial covers a time frame of about 18 months: once eligible patients (adults aged 18 to 65 years, with a BMI between 30 and 45 kg/m2) are identified, 250 will be enrolled and undergo a 12-month observation period following the first visit. During this time frame, there will be a weight loss check after 6 months and a subsequent verification of further weight loss and/or maintenance of weight achieved at month 12. On this point see *DTxO, from Theras Lifetech and Advice Pharma the first digital therapy for the treatment of obesity*, via *www.advicepharma.com*

[29] Here again the reference is to *Terapie digitali, un'opportunità per l'Italia*, in *Tendenze Nuove*, L. Da Ros, G. Recchia, G. Gussoni *et a*l, *ut supra*.

IIa;[30] insofar, neither those belonging to the higher risk classes, which will therefore undergo a more rigorous pathway, nor those that do not have medical characteristics or that perform a mere support function regarding the therapy are included among the devices that benefit from reimbursement.[31]

The path initiated by the DVG aims to enable an ever-widening range of beneficiaries to benefit from the prescription and reimbursability of DiGAs, with an investment in digital-health innovation of €200 million per year until 2024[32] and more than 500 DiGAs submitted for BfArM approval as of March 2022, of which 21 are officially authorized and reimbursed.[33]

As for the rest of the European Union, several countries are following in Germany's footsteps. First among them was Belgium, which, in February 2020, formed an internal working group at the National Institute for Health and Disability Insurance (NIHDI) for the development of DTx reimbursement procedures. The outcome of that study is the so-called mHealth validation pyramid,[34] which presents all the requirements that the digital therapeutics being evaluated must possess, namely:

- Compliance with CE mark and EU Data Protection Regulation 679/2016 (GDPR), with assessment by the Federal Agency for Medicines and Health Products (FAMHP), belgian pharmaceutical regulatory body;
- Adequacy of the digital device in terms of data security and confidentiality, connectivity and interoperability;
- Clinical and socioeconomic demonstration of the added value of DTx over ordinary treatment.

If the therapy being evaluated passes all the steps in the mHealth pyramid, NIHDI provides for its reimbursement by insurance companies. To date, 34 digital therapies have achieved reimbursability in the country through this system.[35]

Finally, France is also showing some interest in Digital Therapeutics. Inspired by Belgium, France is drawing its attention to the requirements that DTxs must meet in order to obtain certification and reimbursability at the insurance level,[36] but with the aim of still ensuring a German-inspired fast-track. The French regulations will come into full effect by the end of 2023, but as of today Insulia, a DTx manufactured by Voluntis for the management and treatment of type II diabetes, is already on the official list of reimbursable health products and services.

5. *Future prospects: potential obstacles to development*

What has been analyzed so far allows us to draw an initial assessment of the impact of digital therapies on health systems, starting from the fact that almost everywhere there is a growing interest in this new type of treatment. Nonetheless, in order to understand the reasons underlying the slowness and/or distrust in the implementation by some States and to promote awareness of the benefits associated with these devices, it is necessary to pinpoint the barriers to development that exist today.

First of all, the absence of clear and shared legislation on the subject represents a gray area that is not entirely insignificant, since the regulation of processes and standards is left to the individual States and this leads to great fragmentation, differences in discipline and often also increases costs and development delays. In Europe this obstacle could be bypassed, for example, with the adoption of a centralized approval process such as to make transposition in the individual Member States more streamlined and automatic.

Secondly, the aforementioned regulatory fragmentation is also reflected in the absence of precise guidelines on reimbursement. This certainly represents the greatest barrier, because it is unimaginable ad unacceptable to think of the approval of any digital therapy in the absence of the relative reimbursement: in

[30] The combination of UE Regulation 745/2017 art. 51 and Annex n. VIII resumes and partially modifies the distinction between medical device risk classes already regulated by the Directive 93/42/EEC.

[31] M. Roehl, *DiGA – Digital Therapeutic Health Application*, in *Allied Clinical Management*, March 2022: "to be defined as a DiGA in Germany it cannot be used exclusively to collect data from a device or for controlling a device, thus it must be used to support the recognition, monitoring, treatment or alleviation of disease or the recognition, treatment or alleviation or compensation of injuries or disabilities".

[32] Source: Federal Ministry of Health, via www.bundesgesundheitsministerium.de/en/digital-healthcare-act.html.

[33] M. Roehl, *ut supra*.

[34] To better understand, see *https://mhealthbelgium.be/*

[35] J. Stevovic, *Terapie Digitali (DTx): framework disponibili in Europa, UK e Stati Uniti*, in *Digital Health Italia*, August 2022.

[36] Vetted by Haute Autorité de Santé (HAS).

Italy, for example, the failure to reimburse digital therapeutics would entail the risk of creating inequity in access to equal or more effective tools, an unacceptable outcome in a universalistic system such as the Italian one.[37]

Undisputedly, all these problems track back above all to a cultural approach still linked to an old conception of medical science, which does not always prove capable of applying the available technological advances: this can be seen both in the poor knowledge of the clinical-validation procedures, which should be more widely shared to promote a full understanding of the phenomenon, as well as in the reluctance of some governments and companies to implement due to the costs and resources (technological and human) to be used in development. If this is accompanied by lack of familiarity with the technology by a part of the healthcare personnel entitled to prescribe such devices, it is easy to understand why digital therapies have not yet reached full diffusion.

Obviously, the hope is that the theoretical interest in these therapies will be accompanied by a concrete commitment to their development. As analyzed in previous paragraphs, digital therapeutics placed on the market have demonstrated clinical efficacy equal to or even superior to the corresponding therapeutic treatments, thus representing a valid alternatives or replacements especially in cases of particularly serious adverse effects or pathologies involving social stigma. Furthermore, the greater active involvement of patients in the treatment required by the therapies – whether by entering data and sending feedback, or by actively participating in games and quizzes – on one hand ensures greater responsibility, also in terms of cost of therapy, and on the other, increased compliance. This positive aspect is particularly appreciable if we consider that one of the most significant problems that apps in general are faced with is precisely the so-called retention, or the ability to retain the customer (patient in this case).[38]

Perhaps the most evident and impactful potential for health systems deriving from the use of digital therapeutics is represented by de-hospitalization: the possibility of preventing or managing a pathology with the aid of a software, which can be used on any digital device at any time of the day and in any place, allows clinicians to concretely guarantee continuity of care and treatment pathway, which is one of the cornerstones and objectives of modern medical science. This, in fact, allows to continue the treatment paths outside the structures, with a strong reduction of costs for the system, more space for acute pathologies or those that require non-replaceable intervention and a different perception of the treatment by the patients, who include it in their daily routine being able to lead a regular life outside the hospital. For this purpose, it would be desirable for individual countries to demonstrate their sensitivity on the subject, proposing courses and technological-education pathways both for healthcare personnel and, especially, for patients, in order to allow anyone actual access to these therapies, which necessarily passes through the understanding and ability to use them.[39]

Hence the development of digital therapies is not free of obstacles and risks. First and foremost, as mentioned, inadequate training of healthcare personnel can lead to counterproductive effects in the care of patients, whose course of treatment could even be slowed down and/or worsened if not properly set up and followed up.

Analogously, poor attention to cybersecurity issues could lead to serious data breaches related to sensitive data entered by/on patients. It is precisely this aspect that is of greatest concern, as evidenced by the healthcare world's focus on insurance solutions to protect against this risk in view of the increasingly-frequent attacks on IT facilities and systems.[40]

[37] In other words, if digital therapies are approved and certified as alternatives or substitutes for traditional therapeutic treatments for which the National Health System (SSN) provides reimbursement, this means that the reimbursement regime must be analogously extended to these new therapies.

[38] A 2019 *Localytis* study reports that nearly one quarter of users abandon an app after just one use and that 62% of users use an app less than 11 times in their lifetime. Source: G. Tripodi, *Un utente su quattro abbandona le app dopo un solo utilizzo*, in *Smartworld*, March 2019.

[39] We are therefore linked to a concept of health *literacy* in the broadest sense.

[40] In this regard, it can be unarguably stated that, with respect to this risk, the insurance market is characterized by hard-market conditions, i.e., increasing premiums and shrinking insurance coverage capacity. This situation is mainly found as a result of the increase in the number of claims in a certain field and is indicative of the rigidity of the system, which struggles to meet the high demand due to a restricted and/or very expensive supply.

Nevertheless, both the potential and the critical issues that have emerged during the pandemic, linked to the growing needs expressed by health systems and populations, point out that the only viable path for health seems to be the one traced out by digitization: in this sense, Digital Therapeutics represents the goal to pursue.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 211-220
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 16

*Public and Private Participation in Digitalised Healthcare**

Maurizio Campagna
(Dottore di ricerca in Diritto pubblico e Professore a contratto di Diritto regionale nell'Università degli Studi di Milano Bicocca)

ABSTRACT The digitalization of health services does not represent a neutral revolution on the regulatory front. In fact, the new digital health will be increasingly populated by private actors, who might not be directly involved in the delivery of health services. In many cases, private entities are the mere holders and developers of the technologies and knowledge that enable the digital transformation of healthcare, without being involved in the care processes, unlike current affiliated healthcare professionals or private hospitals. The engagement of these new actors results in an increased use of soft law as a method of regulation, a trend that has been part of the healthcare system for long and is now being consolidated. However, at the same time a new trend is rapidly emerging: the engagement of private entities in the governance of a system that is becoming increasingly horizontal. This work describes the new relationships between public and private actors in the health sector under the perspective of regulatory requirements.

1. *Opening remarks*

Any reflection aimed at outlining possible future scenarios for a specific public policy area today must begin with an analysis of the contents of the National Recovery and Resilience Plan (henceforth also NRRP), which defines the reforms and investments eligible for funding under the *Next Generation EU Framework.*[1]

With specific reference to the health sector, the NRRP identifies four critical structural aspects of the National Health Service (NHS), which were already clearly evident at the onset of the pandemic: (i) the persistence of significant local disparities in the provision of services, particularly in terms of local prevention and assistance; (ii) a level of integration between hospital services, local services and social services that remains inadequate; (iii) long waiting times for the provision of certain services; (iv) a poor ability to achieve synergies in the definition of strategies for responding to environmental, climate-related and health risks.[2]

The response to these structural criticalities is defined in "Mission 6 Health" of the NRRP, which, in turn, is structured into two components, eight investment projects and two sectoral reforms. The plan for a new NHS outlined in Mission 6 is anchored on three main pillars: the strengthening of local-community care according to proposed organisational models and structures aimed at enhancing proximity of care and home care in particular; the promotion of innovation and digitalisation, also with a view to enhancing service provision by implementing remote-care practices (so-called telemedicine); support for research.[3]

Consistent with the global European recovery project, the achievement of these objectives and, ultimately, the revitalisation of the NHS is entrusted in large part – directly or indirectly – to the opportunities offered by technological development and digitalisation. It is no coincidence that the term "digitalisation" is used no less than nine times in the Mission 6 text, including once in the title of Component 2 – *Innovation, Research and Digitalisation of the National Health Service*, while the word *digital* appears 20

* Article submitted to double-blind peer review.

[1] The Next Generation EU is the European Union's economic recovery instrument for Member Countries following the Covid-19 health crisis; it was enacted by Council Regulation (EU) 2020/2094 of 14 December 2020. The instrument is financed to the limit of EUR 750 billion at 2018 prices.

[2] NRRP, 225. The Plan also highlights that "The Covid-19 pandemic has confirmed the universal value of health, its nature as a fundamental public good and the macro-economic relevance of public health services. Overall, the National Health Service (NHS) shows adequate health outcomes and high life expectancy at birth despite the fact that healthcare expenditure relative to GDP is lower than the EU average".

[3] This summary is proposed by A. Pioggia, *La sanità nel Piano Nazione di Ripresa e Resilienza*, in *Giorn. Dir. Amm*., 2, 2022, 166. The Author proposes a critical analysis of the objectives of Mission 6, in particular highlighting the possible negative repercussions of the development of domiciliary care in terms of inequality. In this regard, see also G. Razzano, *La missione salute del PNRR: le cure primarie, fra opportunità di una "transizione formativa" e unità di indirizzo politico e amministrativo*, in *Corti Supreme e Salute*, vol. 2, 2022, 495 et seq.

times.

Digitalization, which is both a goal and a constituent element of each NHS development and relaunch trajectory, is also functional in ensuring the integration of successful health sector outcomes in the overall systemic recovery plan scenario.[4]

Albeit at the risk of excessive simplification – digitalised healthcare practices or "e-Health" can be identified with the application of ICT to the health sector in order to provide prevention, diagnosis and treatment services, monitor diseases and promote healthy lifestyles. But healthcare digitalisation is not limited to the spectrum of technology applications, it also underpins the innovation of services and how they are delivered. One of the most disruptive outcomes of what is already a manifestly advanced revolution is certainly the profound change it has brought about in the relationship between public and private health-service provision.

Indeed, digitalisation is populating the NHS with a multitude of private entities, owners, operators, and e-Health technology creators, not necessarily involved in healthcare provision, as are the private entities present in the system today: licensed healthcare facilities (clinics and nursing homes), affiliated pharmacies, private Scientific Hospitalisation and Care Institutes (in Italian, the IRCCSs – Istituti di Ricovero e Cura a Carattere Scientifico), affiliated healthcare professionals (General Practitioners and Primary Care Paediatricians).

Our public authorities are thus obliged to rethink a healthcare *governance* model built and consolidated on a public-private relationship paradigm that will soon no longer be the sole option. Sector regulation will, therefore, have to guarantee the NHS from interference by private interests other than the usual ones while simultaneously addressing old and new risks to patients, most notably the *cardinal risk*, namely the vulnerability of their privacy.[5] But as the State takes up its role as regulator of digital technology, it will also have to contend, not only in healthcare, with an unprecedented tendency of new private actors: the latter, in fact, by their sheer size, structural complexity, and the extent of the user base they serve, sometimes act as veritable public authorities in their own right, potentially in competition with the "official" ones.[6]

A struggling legislature[7] is thus facing the challenge of addressing innovation at a time when the NHS, weakened by more than a decade of spending restraint policies[8] and the pandemic, appears severely inequitable, in distress and exposed to new threats.

[4] The centrality of digitalisation is common to all the Missions. Article 18 of Regulation (EU) 2021/241 of the European Parliament and of the Council establishing the recovery and resilience mechanism, envisages that at least 20% of the National Recovery and Resilience Plan budgets must be invested to facilitate the digital transition or to deal with the resulting challenges (Article 18, par. 4, point f). Italy, which plans to allocate 25.1% of its total resources (approx EUR 48 billion) to digitalisation, has therefore adhered to this minimum with considerable margin.

[5] The expression is by C. Casonato. The Author highlights the ambivalence of some constitutional provisions that can promote new technologies and, at the same time, provide protection against their excessive or distorted use. "Thanks to the use of AI, in fact, an otherwise unmanageable volume of data can be processed quickly and accurately to configure highly detailed individual profiles. This clearly reveals the generalised risk of a widespread and pervasive intrusion into the most intimate spheres of each individual, with the risk of a blatant violation of the right to privacy and the exposure of highly personal information that could be used in multiple future situations, from mortgage applications to job interviews or the assessment of social dangerousness risk (the Italian "pericolosità sociale")". V. C. Casonato, *Costituzione e intelligenza artificiale: un'agenda per il prossimo futuro*, in *BioLaw Journal – Rivista di BioDiritto*, vol. 2, 2019, 719. This risk appears to be greatly amplified by the application of new technologies to the health sector, where much of the personal information processed relates to individuals' health and is, therefore, not only extremely sensitive but also the potential target of strong commercial interests.

[6] On this issue, the comment by Facebook founder and CEO Mark Zuckerberg is particularly insightful: "In a lot of ways, Facebook is more like a government than a traditional company". In an interview with journalist Ezra Klein, Zuckerberg he explains the meaning of his statement. https://www.vox.com/2018/4/2/17185052/mark-zuckerberg-facebook-interview-fake-news-bots-cambridge.

[7] Evidence of the difficulties faced by lawmakers in materially addressing technological-innovation issues is manifest in the generic character of the clauses contained in, for instance, Regulation (EU) 2016/679 (the so-called GDPR), Regulation (EU) 2022/2065 (the so-called Digital Service Act), and the proposed European Artificial Intelligence Regulation. This would allow a measure of regulatory free rein to private actors "[...] who are accorded sufficient leeway that, by establishing codes of conduct or standards, can produce legal effects both in respect of those who intend to adhere to them and those who do not". V.N. Maccabiani, *Co-regolamentazione, nuove tecnologie e diritti fondamentali: questioni di forma e sostanza*, in *Osservatoriosullefonti.it*, 3, 2022, 83.

[8] Cf. A Pioggia, *La sanità italiana di fronte alla pandemia. Un banco di prova che offre una lezione per il futuro*, in *Diritto pubblico*, vol. 2, 2020, 385-403.

2. *Public and private healthcare in "analogue mode": overview*

In a public-intervention context, healthcare has historically been markedly polarised, if not outrightly *conflictual*. With regard to the evolution of the entire welfare system itself: *"*on the whole, it has been influenced by three factors, with various degrees of conflict and integration applicable to the various cases: the interaction between the State and the Catholic Church; relationships between public and private sectors; and the relationship between the hub and the outlying structures of our political-administrative system".[9] Before examining the main changes that digitalisation is bringing to the framework of public-private relations, we should review the current situation also from a historical perspective.

Since its establishment by Italian Law no. 833 of 23 December 1978, the NHS has envisaged the coexistence of public and private healthcare providers. Over time, if anything, we have witnessed a change in the degree of integration of the private sector and its quantitative presence in a service that has retained its public character. The constitutional health protection programme itself, as defined in Article 32 of the Constitutional Charter, is fully compatible with such coexistence. The law specifically mandates the Republic to protect health, without, however, stipulating that services be public entities or allocating precise areas to their control, but instead leaving room for the development of mixed systems. It is quite true that public entities are called upon to intervene with greater responsibility.[10] Indeed, the presence of private providers could even be considered necessary because it is instrumental in guaranteeing patients the freedom to choose their healthcare practitioner and facility, between available modes of treatment and techniques, and between different care and rehabilitation programmes.[11]

The relationship between public and private actors in the healthcare system has undergone profound changes, coinciding with the key *institutional junctures*[12] of the NHS.

[9] G.L. Bulsei, *Il servizio sanitario nazionale tra decisioni politico-amministrative e pratiche sociali*, in R. Balduzzi (ed.), *Trent'anni di Servizio sanitario nazionale. Un confronto interdisciplinare*, Bologna, Il Mulino, 27.

[10] Cf. D. Morana, *Tutela della salute,* in G. Corso, V. Lopilato (ed.), *Il diritto amministrativo dopo le riforme costituzionali*, *Parte speciale*, vol. 1, Milan, Giuffrè, 2006, 266. On the same theme, see R. Ferrara, *Salute (diritto alla)*, in *Digesto discipline pubblicistiche*, Turin, Utet, XIII, 520, according to which "it would be plausible to believe that the Constituent Assembly wanted to outline and frame the healthcare-related duties of the Republic in the manner of other public functions, i.e. functions in the strict sense that cannot be divested since their exercise cannot be broken down into parts given that they are connected to and implicit in the very foundations and grounds of the welfare state based on the rule of law". See also the arguments posed by R. Balduzzi and D. Servetti. The Authors assert that "[...] the Republic's duty to safeguard its citizens as mandated by the Constitution is inalienable and, as such, the actions of public authorities in the field of healthcare override those of private interests [...]". V.R. Balduzzi e D. Servetti, in R. Balduzzi, G. Carpani (ed.), *Manuale di Diritto sanitario*, Bologna, Il Mulino, 26.

[11] Cf. F. Toth, *Le politiche sanitarie*, Roma-Bari, Laterza, 2009, 57. The Author focuses on how each healthcare model addresses a diversity of subjects and breadth. Following recent regulatory initiatives, freedom of choice is recognised as both an expression and consequence of the centrality that the legal system has acknowledged to the value of trust in the care relationship. Italian Law no. 217 of 22 December 2019 – *Rules on informed consent and advance medical treatment decisions* establishes the role of informed consent in healthcare. In Article 1, par. 2, it states that "the relationship of care and trust between patient and doctor is fostered and valued; it is based on the principle of informed consent, which jointly envisages the decision-making autonomy of the patient and the skill, professional independence and responsibility of the doctor. Healthcare professionals who make up the healthcare team contribute to the care relationship, according to their respective skills. If the patient so wishes, the relationship is extended to include his or her family members, civil partner or cohabitee, or a person of trust.". In the aftermath of the approval of the first law on informed consent in healthcare, it was asserted in the literature that "The reference to trust is important because it "enfolds", so to speak, the core of the care concept, and contributes to excluding any technical reductionism of the term "care" itself. Significant, albeit coincidental, is the repetition of the term "trust" for a different purpose in the remainder of the provision, which states that "If the patient so wishes, the relationship is extended to include his or her family members, civil partner or cohabitee, or a person of trust". Also this allowance for "inclusion" in the relationship helps to clarify the role of the patient's "carers" by establishing a "multiparty" relationship: which does impact the consequences for what we jurists refer to as the prerogatives of each individual". V. P. Zatti, *Spunti per una lettura della legge sul consenso informato e DAT*, in *La nuova giurisprudenza civile commentata*, vol. 1, 2018, 247.

[12] The expression was coined by A. Mattioni, who outlined the historical evolution of the NHS marked by its institutional junctures corresponding to the four national healthcare reforms: Italian Law no. 833 of 23 December 1978, Italian Legislative Decree no. 502 of 30 December 1992, Italian Legislative Decree no. 517 of 7 December 1993 and Italian Legislative Decree no. 229 of 19 June 1999. "Institutional innovation calls for a response that must empower an appropriate framework of healthcare governance, inclusive of new activities that can safeguard it and enhance its conceptual configuration [...]". This message can also apply today, at the

In the original scheme foreseen by NHS constituent law no. 833/1978, private providers were restricted to a function of mere support to public structures in the cases – which were expected to be rare – in which the latter would be unable to guarantee adequate coverage.[13] Indeed, the fruition of hospitals and outpatient facilities managed by the Local Healthcare Units (in Italian USLs – Unità Sanitarie Locali) was also promoted with a view to safeguarding and enhancing public investment while at the same time curtailing private entrepreneurial interests. This rigid original dualism, therefore, envisaged public-service provision under public administration governance, while private institutions could only enter as licensees of the service,[14] according to very strict entry rules.

This arrangement, as we know, was superseded by the reforms of the early 1990s (Italian Legislative Decree no. 502 of 30 December 1992 and Italian Legislative Decree no. 517 of 7 December 1993). The USLs were transformed into Local Health Enterprises (ASLs – Aziende Sanitarie Locali) on a provincial or sub-provincial basis and vested with organisational, administrative, financial, accounting, management and technical autonomy. In addition to providing healthcare, the ASLs were empowered to outsource services, thus extending their roles from mere "producers" to being "clients" of services as well. The essential levels of care would have been guaranteed not only by the operations of public facilities directly managed by the ASLs[15] but also by private institutions in return for the payment of scheduled fees for each type of service provided. Every patient would also have been guaranteed access to private providers, on condition that the latter were licensed, thus better guaranteeing individual freedom of choice (see Article 8-bis of Italian Legislative Decree 502/1992, as amended by Italian Legislative Decree 229/1999).

In a nutshell, licensing (or accreditation) entails a system whereby private facilities may provide services no longer only in their own name, but also on behalf of the NHS, within the limits set by sector planning and on the basis of specific agreements with the locally-competent health authorities, under the governance of the NHS: "In essence, the healthcare service should be managed according to a principle of fair competition between public and private entities".[16] The accreditation process imposes specific additional requirements beyond those mandated by the authorisation procedures applicable to licensees that establish and operate healthcare facilities; operators must comply with regional planning guidelines and successfully pass audits of their activities and achieved results.[17]

The public-private framework laid down in the 1990s remained virtually unchanged until the 1999 reform (Italian Legislative Decree 229 of 30 June 1999), which – as we know – completed the so-called corporatisation of

height of the digital revolution. V. A. Mattioni, *Le quattro riforme della sanità. Una lettura sinottica di snodi istituzionali*, in R. Balduzzi (ed.), *Trent'anni di Servizio sanitario nazionale. Un confronto interdisciplinare*, Bologna, Il Mulino, 2007, 263.

[13] V. A. Pioggia, *Diritto sanitario e dei servizi sociali*, Giappichelli, Turin, 2014, 123. On this subject, see also A. Catelani, *La sanità pubblica*, in G. Santaniello (ed.), *Trattato di Diritto Amministrativo*, vol. XIV, Milan, Cedam, 2010, 153-154.

[14] On this subject, see G. Corso, *Pubblico e privato nel sistema sanitario*, in G. Corso, P. Magistrelli (eds.), *Il diritto alla salute tra istituzioni e società civile*, Giappichelli, Turin, 2009, 19-20. According to the Author, "It is clear that the role of the private sector is marginal in this design".

[15] Paragraph 5 of the original version of Article 8 of Italian Legislative Decree 502/1992 laid down that the USLs assure citizens the provision of specialised services, including rehabilitation, instrumental and laboratory diagnostics, and hospital services by availing itself *"*of its own facilities, as well as of the enterprises referenced in Article 4 [hospitals], of public health institutions, including military or private hospitals, in addition to public facilities […]*"*.

[16] V. G. Fares, *Problemi attuali dell'ordinamento sanitario*, Editoriale Scientifica, Naples, 2012, 59. On the subject, see also, V. Molaschi, *Autorizzazione, accreditamento e accordi contrattuali tra esigenze di contenimento della spesa pubblica e tutela della concorrenza (Nota a Cons. Stato sez. III 16 settembre 2013, n. 4574)*, in *Giurisprudenza italiana*, vol. 3, 2014, 675; V. Molaschi, *Tutela della concorrenza, vincoli di spesa e rapporti tra Servizio sanitario nazionale e soggetti privati: una riflessione alla luce della modifica del titolo V della Costituzione (nota a TAR Lombardia, Milano, sez. I, 29 ottobre 2003 n. 4899),* in *Foro amministrativo TAR,* vol. 5, 2004, 1271.

[17] In its judgment no. 195/2021, the Constitutional Court described the system as follows: "The healthcare system, as reformed by legislative decree no. 502 of 1992 and then significantly remodeled by Italian Legislative Decree no. 229 of 1999, defines the public-private healthcare provision relationship according to a progressive system, on the basis of which entities intending to provide healthcare services must be authorised; if compliant with this as a prerequisite, they can apply for institutional accreditation, which renders them potential providers of healthcare services on behalf of the National Health Service. This step must be preceded by the stipulation of contracts with the administration and respect of the spending limits set out therein".

healthcare that had begun in the early years of the decade.

In the context of the new relationship briefly outlined, governance and regulatory efforts have been substantially oriented in two directions: on the one hand, to ensure that private providers functionally contribute to the fulfilment of the NHS statutory mission on the basis of the rules, especially regional rules, on accreditation; on the other hand, and to a preponderant extent, to control private expenditure, by means of a series of progressively-introduced mechanisms, including planning, expenditure limits defined for each provider,[18] and regressive rates,[19] to mention the main ones. Governance, therefore, has so far focused on two fundamental aspects: the entry of the private sector into the system and the control of the expenditure it generates. This mode of governance, however, is effective only on the condition that private entities provide healthcare.[20] The risk to be prevented or contained, in this case, is mainly the provision of inappropriate care, which in turn generates inappropriate expenditure, i.e. not properly invested in healthcare endeavour.

Acquired tools and expertise, therefore, cannot be exported *outright* to regulate the participation of new private operators who are not directly involved in care and assistance but who do possess knowledge, infrastructure and economic capacity for research and development in digitised healthcare.

The "accreditation system" and its general requirements, however, must be extended to the new digital health services and performances, in order to guarantee not only appropriateness and functionality with respect to the objectives of regional planning. The accreditation of digitised healthcare must, in fact, also be aimed at guaranteeing the technical safety of the services and the general compliance of the services with the regulatory apparatuses aimed at preventing the new risks: above all, the most relevant are those for the privacy of the patients and those for cybersecurity. The document "National Guidelines for the Provision of Telemedicine Services", approved by the State-Regions Conference with the agreement of 17 December 2020, contains some clear guidelines in this regard. Particular attention is paid to the technical training of personnel who will be responsible for providing telemedicine services: specific accreditation requirements are envisaged. A trained staff is certainly better able to contribute to the safety of the services.

3. *The private sector in the digital healthcare domain and the need for a new regulatory framework*

Whereas the contribution of private healthcare entrepreneurs could be regarded as supplementary to public provision (presumably capable of covering the need for healthcare), the participation of entrepreneurs from the digital sphere, on the other hand, is necessary: suffice it to mention the availability of data-storage infrastructure, an essential

[18] See recently, Campania Regional Administrative Court, decision no. 976 of 13 February 2023: "[...] the determination of expenditure caps is the expression of a regional planning power characterised by broad discretion in forecasting the extent and mechanisms for allocating the available resources, with the aim of balancing multiple and often conflicting interests of constitutional relevance, such as the containment of expenditure on the basis of the resources effectively available, the need to ensure quantitatively and qualitatively adequate healthcare services to patients, those of private structures operating on an entrepreneurial basis, and those of public structures tasked with providing services in compliance with the principles of efficiency and sound management".

[19] In Judgment no. 3809 of 20 June 2018, Section III of the Council of State asserted, "The regressive rate system implemented by the healthcare services (RTU – Regressione Tariffaria Unica) is the mechanism through which the Regional Authorities, called upon to plan and budget their relevant expenditure, ensure compliance with the ceilings assigned to them as well as overall organisational and financial stability. In other words, the "regression" mechanism enables the Regional Authorities to refund their treasuries with the monetary amounts related to healthcare services provided by accredited private facilities that exceed maximum limits established under the powers vested in public controllers of healthcare spending. It is therefore a method of final and contingent adjustment and rebalancing with respect to advance budgetary planning [...]".

[20] Private entities that are an integral part of the NHS also include General Practitioners and Primary Care Paediatricians. These professionals are retained under the affiliation system, which defines rights and obligations vis-à-vis the public service (organisation of outpatient activities, number of hours to be guaranteed, remuneration, incentives). Also in this case, private entities participate in the NHS and cater for a share of the healthcare provision. There is a high concentration of private entities within the pharmaceutical distribution network, which fully falls under the concept of healthcare. The reference is to privately owned local-community pharmacies, which are also affiliated to the SSN. Lastly, the private Scientific Hospitalisation and Care Institutes (IRCCSs), albeit pursuing research activities as one of their statutory purposes, are engaged in healthcare activities in the same way as hospitals.

resource for mechanisms such as the electronic health record (the Italian FSE – Fascicolo Elettronico) and the platforms that enable the provision of specific services. An excellent example of the aforementioned phenomenon is the recent commissioning of a National Telemedicine Platform by AGENAS, the National Agency for Regional Health Services, to a group of private companies, with the aim of creating "a fundamental level of interoperability capable of enforcing common standards for telemedicine services developed by the Regional Authorities, enhancing what is already available on a local level, supplementing or enhancing the range of provided services". In particular, the planning, implementation and management of the Enabling Services of the National Telemedicine Platform – sub-investment 1.2.3, within Mission 6 Component 1 of the NRP – were entrusted to a temporary consortium of companies that submitted a proposal following the call for expressions of interest published pursuant to Article 183, Paragraph 15 of Italian Legislative Decree No. 50/2016 (Public Contracts Code), which regulates so-called project-financing initiatives.[21] Private entities were therefore entrusted with the responsibility of implementing one of the most salient projects in the revitalisation of the NHS, telemedicine.[22] From a relational framework in which the NHS has always retained a pre-eminence and a dominant position over private actors (also from an ideological perspective), with the onset of digitalisation, the relationship is destined to develop on a basis of greater peer parity. In the absence of effective control and regulation, we could even see a gradual reversal of positions.

The new relationship between the public and private actors is affected by changes in another arena: the confrontation between the State and new technologies. Indeed, for the first time, the latter represent both "an intrinsic aspect of public power and a phenomenon whose regulation is central to economic and social relations as a whole".[23]

For some time now, technologies have been an integral part of the NHS and an integral part of the services provided, not only in the context of projects and activities officially headed by the public service. Also the private use of ICT tools, which has pervaded everyone's daily routine, in some cases synergises with the NHS, sometimes facilitating its operations, at other times supplementing them and improving their effectiveness. Possible ways of facilitating the relationship between users and the SSN include the use of instant messaging apps to dialogue with one's General Practitioner and to share reports and documents. The use of medical apps provided by private health centres, on the other hand, enables the tracing of patient care actions. By allowing their General Practitioners to access such data, patients enable them to supplement information already held by the NHS with that generated and stored by private providers, effectively creating a mixed public and private healthcare database.

The example of the Telemedicine platform,

[21] By resolution No. 423 of 11 October 2022, the National Agency for Regional Health Services (AGENAS) – in its capacity as the implementing party of the sub-investment Telemedicine, Component 1, Mission 6 Healthcare – called an open online tender procedure through the Net4market platform aimed at awarding a contract for the design, implementation, and management of the enabling services of the National Telemedicine Platform. The tender is covered by *project financing* pursuant to Article 183, par. 15 of Italian Legislative Decree 50/2016, with an estimated value of EUR 341,575,855.84 (excluding VAT). The procedure was closed on 8 March 2023 with the award of the contract by Agenas to the Temporary Enterprise Consortium (RTI – Raggruppamento Temporaneo di Imprese) Engineering Ingegneria Informatica S.p.A. and Almaviva S.p.A. The RTI will have to guarantee interoperability with the common components shared with the ESF 2.0 application architecture and with the Health Data Ecosystem, also with the goal of "facilitating the planning, governance and development of digital healthcare". Information on the procedure can be found on the institutional website of AGENAS, in the section "Calls for tenders and contracts": https://www.agenas.gov.it/bandi-di-gara-e-contratti2 (last consultation date: 26 March 2023).

[22] On the subject, see also, among others: C. Botrugno, *Un diritto per la telemedicina: analisi di un complesso normativo in formazione*, in *Politica del diritto*, vol. 4, 2014, 639-668; C. Botrugno, *La diffusione dei modelli di cura a distanza: verso un "diritto alla telesalute"?*, in *BioLaw Journal – Rivista di BioDiritto*, vol. 1, 2014, 163-175; C. Botrugno, *Telemedicina ed emergenza sanitaria: un grande rimpianto per il nostro Paese*, in *BioLaw Journal – Rivista di BioDiritto Instant Forum – Diritto, diritti e emergenza ai tempi del Coronavirus*, 2020; F. Gori, P.G. Macrì, S. Turco, E. Turillazzi, *Telemedicina: da emergenza a nuova normalità. Riflessioni medico-legali*, in *Responsabilità civile e previdenza*, vol. 2, 2021, 69. On the implications of Telemedicine in terms of professional liability, see F. Aperio Bella, *The Role of Law in Preventing "Remote" Defensive Medicine: Challenges and Perspectives in the Use of Telemedicine*, in *Federalismi.it*, vol. 1, 2023, 305.

[23] L. Torchia, *Lo Stato digitale. Una introduzione,* Bologna, Il Mulino, 2023, 19.

on the other hand, illustrates how public authorities and private entrepreneurs can and must collaborate in future scenarios.

Hitherto, the operations of private-sector service providers have been strongly affected by public administration prerogatives, such as determining the extent and types of services contracted, determining their suitability, and ultimately, using such leverage to influence the organisational arrangements of the private facilities themselves. This relational paradigm hinged on a substantively well-founded assumption, i.e. that public health authorities, partly owing to their accrued technical expertise (considering that these are the ASLs, the Local Health Enterprises), can be empowered to discretionally assess healthcare requirements with a view to, on the one hand, protecting the public status of the service and, on the other, containing the affirmation of extraneous private interests. As digitalisation advanced, the private sector stakeholders gained more weight in the relationship also by virtue of their technical expertise, aptitude for research and development, swiftness of response and, in some cases, their extraordinary financial resources.

It has been pointed out in scholarship that *"*in contexts characterised more by horizontal relational dynamics than by hierarchical interactions, and therefore more by participatory forms and output-derived procedural legitimation than by the rules of democratic political representation, it is equally true that in fields where governance prevails, soft regulation models find implementation*"*. The characteristics of so-called *soft law,* moreover, would be well suited to the dynamics of innovation, which are rapid and have very uncertain outcomes: *"*[...] as a potentially transitory mode of rule-making, halfway between the generic indication of policy lines and legislation, it may represent the best approach to tackle complex and diverse problems characterised by uncertainty".[24]

*Soft law, a "*convenient category that subsumes a world of regulatory ectoplasms*",*[25] englobes, among other things, the so-called guidelines, codes of conduct, good practices and standards. This corpus, although lacking the efficacy formally accorded to legislative enactments, is nevertheless capable of influencing the actions and behaviour of actors in certain specific sectors.

In the health sector, *soft-law* precepts have been adopted extensively for some time now, mainly due to the less rigid nature of the rule-forming process and the possibility of involving technical experts.[26]

[24] Similarly, E. Stradella, *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte e le prospettive. Alcuni spunti di riflessione*, in *Media-Laws. Rivista di diritto dei media*, vol. 2, 2019, 78. The Author mainly addresses the themes of artificial intelligence and robotics, but these can extend to the broader scope of digitalization, in including the digitalization of healthcare. See also O. Pollicino, *I codici di condotta tra self-regulation e hard law: esiste davvero una terza via per la regolazione del digitale? Il caso della strategia europea contro la disinformazione online*, in *Rivista trimestrale di diritto pubblico*, vol. 4, 2022, 1051. The Author reviews, among other things, the debate on the regulation of the web, in particular highlighting its polarisation between two distinct positions which, in turn, emerge from two different traditions: on the one hand, the proponents of hard law in Europe and, on the other hand, the promoters of the use of soft law in the United States. The American debate, moreover, has seen the acknowledgement that "the peculiarities of cyberspace were not such as to distract the activities that took place there from any rules of conduct that had not already been introduced by states to govern the 'world of matter'*",* abandoning an initial almost anarchic position whereby the web was considered an unregulated space.

[25] Such ectoplasms are "endowed with varying degrees of regulatory power; where the intensity is not to be measured by the greater or lesser effectiveness of these disciplines, but is determined by the greater or lesser use of sanctioning instruments, falling under the traditional State monopoly*"*. See R. Bin*, Soft law, no law,* in *A. Somma, (*ed.), *Soft law e hard law nelle società post-moderne,* Turin, Giappichelli, 2009, 31-40.

[26] There are numerous examples of alternative regulation, included in the category of *soft law*, already used in the health sector. Among the most well-known and recent, see for example the document *National indications for the provision of telemedicine services,* approved by Agreement approved by the State-Regions Conference of 17 December 2020 (Register of Acts no. 215/CSR). On the regulation of Telemedicine via soft law enactments, please refer to M. Campagna, *Linee Guida per la Telemedicina. Considerazioni alla luce dell'emergenza Covid-19*, in *Corti Supreme e Salute*, vol. 3, 2020, 599. On the regulation of professional enagegment in healthcare, Law no. 24 of 8 March 2017, the so-called Gelli-Bianco bill, in Article 5 states that "Practitioners of healthcare professions, in the performance of healthcare services with preventive, diagnostic, therapeutic, palliative, rehabilitative and forensic purposes, shall comply, without prejudice to the specifics of the concrete case to the recommendations set forth in the guidelines published pursuant to paragraph 3 and drawn up by public and private bodies and institutions, as well as by the scientific societies and technical-scientific associations of the health professions registered in a special list established and regulated by decree of the Minister of Health, to be issued within ninety days from the date of entry into force of this law, and to be updated every two years. In the absence of the aforementioned recommendations, healthcare profes-

Thus, by favouring the use of *soft law* in all its manifestations (including self-regulatory scenarios), digitalisation could fuel the fragmentation of regulatory foundations in the healthcare sector, where governance has long been affected by considerable stratification and regulatory superfluity. The Covid-19 emergency, moreover, contributed to increasing the level of regulatory complexity: a crisis reaction mechanism, in fact, demanded the adoption of *"*a multiplicity of emergency measures, related to both healthcare and economics, [...] generating a veritable regulatory 'epidemic'".[27]

In confirmation of what has been argued here, the opinion of the Council of State (Consultative Section for Regulatory Acts) on the draft decree of the Minister of Health concerning the *Regulation on Models and Standards for the Development of Local Assistance in the National Health Service*, no. 881 of 19 May 2022, is of particular interest. This act is of fundamental importance for the implementation of healthcare-related NRRP initiatives. As we know, the scheme was then definitively approved and was incorporated into Italian Ministerial Decree No. 77 of 23 May 2022.

The Council of State noted that the Regulation submitted for its examination would have been superimposed on "a NHS regulatory framework that has been stratified over a long period of time, now measured in decades, and is highly articulated and complex in its sources, bodies, responsibilities and procedures". The proposed decree, therefore, would only have constituted "a further "regulatory layer" to the others, without replacing or even modifying them, only incrementally increasing the existing regulatory stock".

In this context, whereas soft law seems to be particularly suited to the regulation of technology and thus a somewhat inevitable solution, in literature,[28] it has also been pointed out how the assertion of soft law actually favours two trends: on the one hand, a shift of regulatory power from a national to a transnational domain, and, on the other hand, a contextual stakeholder shift from the public to the private sector (with reference to the phenomena of self-regulation and co-regulation).[29]

4. *Concluding remarks*

The healthcare digital transition is rapidly changing systemic relationships and relations: the relationship between public and private sectors is no exception. The new paradigm – anchored on balances of power and relationships that differ greatly from those of the past – calls for a regulatory framework that secures system governance, thereby updating and effectively implementing foundational NHS principles. This scenario is witnessing the consolidation of a trend that has long been present in the healthcare system, namely the use of *soft law* as a method of regulation. At the same time, however, a new trend is rapidly emerging: the involvement of private entities in the governance of an increasingly horizontal system.

The effectiveness of the new rules will be measured by their ability to provide a clear frame of reference "to enable the State and the

sionals should adhere to good clinical-care practices". Par. 3 of the same Article provided for the establishment of the National Guideline System, whose tasks and functions are regulated by the decree of the Minister of Health of 27 February 2018. The guidelines may be drawn up by public and private bodies, as well as by scientific societies and the technical-scientific associations of the health professions listed in the decree of the Minister of Health of 2 August 2017. Regarding the regulation of organisational models of significant importance for the NHS, we should mention the document "*Revision of the Organisational Guidelines and Recommendations for the Oncology Network that supplements acute and post-acute hospital activity with local activity*", approved with the Agreement approved by the State-Regions Conference on 17 April 2019 (Register of Acts no. 59/CSR). The Regional Authorities, to which the document is addressed, are required to implement the indications of Ministerial Decree 70/2015 – the so-called Hospital Standards – which establishes the rules for the construction of clinical-welfare networks, which include the oncology network. The proposed examples represent how acts with diverse names, but in any case not classifiable as hard law, have been used to regulate also very relevant aspects of the healthcare sector.
Among the numerous examples of alternative regulation concerning organisational models, see for example, the guidelines for the oncological network.

[27] Similarly, G. Napolitano, *Consiglio di Stato e qualità della regolazione tra pandemia e PNRR*, in *Giornale di diritto amministrativo*, 2022, 153.

[28] See again E. Stradella, *La regolazione della Robotica e dell'Intelligenza artificiale: il dibattito, le proposte e le prospettive. Alcuni spunti di riflessione*, 79

[29] On this subject, with particular reference to the European constitutional system, which has favoured the success of such instruments, see M. E. Bortoloni, *La regolazione privata nel sistema costituzionale dell'Unione Europea. Riflessioni sulla disciplina relativa al settore dell'innovazione tecnologica*, in G. Di Cosimo (ed.), *Processi digitali e tecnologie digitali*, Turin, Giappichelli, 2023, 63.

local authorities to adequately supervise the use of these laborious and sophisticated technological processes and tools designed by private entities, in order to remain as guarantors of the constitutional rights to health, social assistance and the principle of equality*",*[30] always ensuring that the use of the new technologies is consistent with the institutional mission of the NHS and that the latter's fundamental principles are respected.

Firstly, the ability of digitalisation to generate inequality is well known, albeit with a new trait. In fact, it does not depend on the level of wealth of individuals. The term "digital divide"[31] refers to existing differences in the possibility of using Internet services, due to age, the presence of adequate infrastructure, and digital culture. In healthcare, it means unequal access to new services, with effects that would compound the systemic structural inequalities. Efforts must therefore be directed at identifying solid equality safeguards that can withstand the pressure of digitalisation. The first obstacle to overcome will therefore be the operational adequacy of Essential Levels of Care (ELC). The procedure for their definition and renewal does not, in fact, appear to be entirely compatible with innovation time frames. Moreover, the structure of the measure that will define them, consisting essentially of a series of lists of services, could prove excessively rigid and unsuitable for configuring digital health services subject to rapid changes and uncertain classifications.

Regulatory interventions will have to act simultaneously on several levels. If one of the main causes of the digital divide continues to be poor knowledge of the new technologies,[32] the digital transition (not only in healthcare) will have to be accompanied by substantial investments in training and education, not only of patients, but also by intervening in schooling.

On the privacy front, the risk for health-service users appears to be much higher than the average risk associated with the use of technologies due to the particularly sensitive nature of the information processed in the provision of digitised care.

Lastly, due consideration must be given to the risk that private interests other than those for which various forms of protection have been developed over the years – such as systems to control the appropriateness of expenditure – will filter into the system, altering the character of the NHS as a public service.

In view of these risks, in the new relationship between public and private sectors – whatever system of regulation is chosen and whatever techniques are employed – the public authorities must resolutely pursue the balancing of diverse interests as an essential vehicle for adapting the framework of constitutional values to the existing and changing reality. This is an indispensable function for the resilience of the system, even when it develops horizontally and thus resistant to "imposed" regulation and more suited to governance by all actors. An effective solution in the management of digitalisation risks themselves can be found in the balancing of interests, which, on the other hand, directly contributes to the identification of such risks as they are directly represented

[30] See also E. A. Ferioli, *L'intelligenza artificiale nei servizi sociali e sanitari: una sfida al ruolo delle istituzioni pubbliche nel welfare italiano?*, in *BioLaw Journal - Rivista di BioDiritto*, vol. 1, 2019, 175. With specific reference to Artificial Intelligence, it has been pointed out in the literature that "the protection of rights appears, indeed, to be only one of the aspects in respect of which it is desirable that an evolution should take place that is capable of restoring a high level of control by individuals. From the perspective of public law, there are also requirements of governance of technology, which imply the need for regulators to implement appropriate forms of consultation at national and supranational levels". V. A. Pajno, M. Bassini, G. De Gregorio, M. Macchia, F. P. Patti, O. Pollicino, S. Quattrocolo, D. Simeoli and P. Sirena*, AI: profili giuridici. Intelligenza artificiale: criticità emergenti e sfide per il giurista,* in *BioLaw Journal - Rivista di BioDiritto,* vol. 3, 2019, 217.

[31] The digital divide "represents one of the most significant causes of social exclusion in contemporary advanced societies. The growing importance that the Web has acquired as an instrument of mediation of social relations makes it possible to configure the possibility of accessing the Web itself (and of conscientiously operating therein by fully exploiting the wealth of knowledge available) as an increasingly indispensable prerequisite for full participation in political, economic and social life and for the full development of the individual's personality. In this perspective – which primarily calls into question Articles 2 and 3, par. 2, of the Constitution – the victims of the digital divide suffer from an obstacle – the extent of which is increasingly manifest every day – that impedes the full development of individuals and deprives them of increasingly essential tools for exercising fundamental freedoms*"*. See also P. Zuddas, *Covid-19 e digital divide: tecnologie digitali e diritti sociali alla prova dell'emergenza sanitaria*, in *Osservatorio di Diritto Costituzionale*, vol. 3, 2020, 285.

[32] The report on the Digitalisation Index of Economy and Society (DESI), edited by the European Commission, notes for the year 2022 that in Italy, more than half of the citizens still do not even have basic digital skills.

in the regulatory texts.[33]

The real challenge therefore seems to be to "stop chasing and start leading", acknowledging that the digital revolution has already taken place. If this is the time for *design*, i.e., the time to define a human model for the digitalised world, the ultimate challenge lies in the governance of the digital reality (deciding what we want to do with it) and establishing methods and tools for its regulation.[34] The protection of health, given its centrality in the human journey, perhaps requires greater caution and urgent action. Precisely because of its inherent complexity, the healthcare system appears, once again, to be an extraordinary test bed.

[33]See, for example, the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain legislative acts of the Union COM(2021)206 final. In the context of the proposal, it is quite clear that the goal of managing risks arising from artificial intelligence has permeated text drafting techniques and systems. On the subject, see C. Casonato, B. Marchetti, *Prime osservazioni sulla proposta di regolamento dell'Unione Europea in materia di intelligenza artificiale*, in *BioLaw Journal - Rivista di BioDiritto*, vol. 3, 2021, 415.

[34] Cf. L. Floridi, *Ethics of Artificial Intelligence*. *Developments, opportunities, challenges*, Milan, Raffaello Cortina Editore, 2023, 123 et seq. The Author, referring to all technologies and not only to AI, examines various regulatory drivers and makes a clear distinction between governance, regulation and ethics as they apply to digitalisation. The first "is the practice of establishing and implementing policies, procedures and standards for the correct development, use and management of the infosphere". Digital regulation, on the other hand, is "relevant legislation, a system of laws developed and enforced through social or governmental institutions to regulate the behaviour of relevant agents in the infosphere". Finally, digital ethics is "that field of ethics that studies and evaluates moral issues related to data and information (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including AI, artificial agents, ML and robots) and related practices and infrastructures (including responsible innovation, programming, hacking, professional codes and standards), in order to formulate and support morally good solutions, e.g. sound conduct or good values". It is thought to be digital ethics that would shape digital regulation and digital governance "through a moral assessment of what is socially acceptable or preferable". In a series of public statements, the author recently confirmed his position on the measure reported by the Italian Data Protection Authority on 30 March 2023 (Register of Measures no. 112 of 30 March 2023) which ordered the provisional restriction on the processing of personal data of data subjects established in Italy against OpenAI L.L.C., a US company that develops and operates ChatGPT, in its capacity as the data controller responsible for the processing of personal data carried out through that application. The measure caused a lot of uproar and triggered a lively debate on whether innovation should be impeded or, rather, governed by rules that incorporate ethical principles. See https://www.huffingtonpost.it/economia/2023/04/01/news/luciano_floridi_chat_gpt_garante_privacy-11725205/ (last consulted 1 April 2023).

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 221-231
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 17

*Digital Demands: An Overview of the Journey Toward Access and Reimbursement in the German Statutory Health Insurance**

Simone von Hardenberg
(Professor at University of Applied Studies Munich)

Lauren Tonti
(Doctoral Candidate at Max Planck Institute for Social Law & Social Policy)

ABSTRACT Digitization is inherent to the technological innovation in the future of health care, and relatedly, health-insurance coverage. It also makes inherent demands upon healthcare systems. Germany has long sought to incorporate the ever-changing elements of digitization into its system services and structures. This paper explores the development and status of digitization in the German statutory health-insurance system. After first providing the context of the system in which digitization is occurring, the paper provides an overview of significant legislative efforts to promote digitization in the healthcare sector. It highlights the German experience with integrating digital health applications into the statutory health-insurance system as an example to illustrate the challenge of implementing new digital services in German healthcare, before offering considerations for the future.

1. *Introduction*

The future of healthcare is inherently linked with digitization. Systematic collection and analysis of medical data improves the detection of diseases, enables personalized therapies, and reveals new healing opportunities. Digitalized healthcare can also help address current access challenges facing elderly and chronically-ill patient populations, or patients located in geographically-remote or otherwise disconnected areas. Digitization enables easier communication between the many actors in the healthcare system who together make up and coordinate a patient's care. Digital technologies can strengthen patients' self-determination and health competency. Combined, these benefits contribute to maintaining and further developing high-quality care in face of rising healthcare costs.

Digitization also makes inherent demands upon healthcare systems that may hold varying degrees of readiness for integrating digital instruments and services. Digitization is seen as a potential instrument for optimizing healthcare processes and developments, which occur in nearly every country. While there exists no single uniform definition of digitization or e-Health, a term used equally as broadly and indiscriminately, there is a common understanding that systems should leverage the benefits and potential of digital-health technologies to the maximum possible.

The German experience of integrating e-Health activities has been prolonged and intentional. Often discussed in the media, debated in halls of the legislature, or even criticized in patient-exam rooms, the experience of the system's approach to digitalizing Germany's healthcare sector is useful to analyse, for examining the series of changes in pursuit of digitization, and the inherent challenges encountered in the pursuit thereof, offers valuable lessons. Insight gleaned from this journey can serve as a model and inspiration for other systems seeking to tackle the monumental task of incorporating e-Health and its many facets into their systems.

Accordingly, this paper provides a brief but broad overview of the actions toward developing e-Health in the German health system. With a focus on ambulant healthcare[1], it first explains the legal framework and the landscape in which digitization is occurring, then traces significant legislative action over the last two decades before highlighting prescription digital-health applications as an

* Article submitted to double-blind peer review.

[1] The discussion excludes long-term healthcare and rehabilitative services.

example of digitization in practice in the German healthcare system.

2. *Digitization in the German Statutory Health Insurance System*

2.1. *Digitization in Context: The German Healthcare System*

The context of the system and environment in which digitization is intended is relevant not only because of the number of patients affected, but also because legal guarantees regarding the provision of healthcare must be observed. The technological capabilities enabled by digital innovations are integral to provide economic but high-quality care. Briefly explaining the statutory health-insurance (SHI) context helps explain the national journey toward digitization.

2.1.1. *Statutory health insurance*

Digitization can only fulfil its potential when it can be successfully integrated into the healthcare system, whether through existing channels or legislative reforms.

A statutory health-insurance (SHI) system that insures nearly 90 per cent of the population predominates the German healthcare landscape.[2] While private health insurance coexists and operates in the system, it covers a much smaller percentage of the population, and the insured cannot easily alternate between SHI and private insurance. Book V of the German Social Code ("Sozialgesetzbuch V", SGB V) contains the legal requirements that provide structure to and guide the system, which has traditionally been characterized by a strict separation of ambulatory and hospital care.

The SHI is a compulsory insurance. The SHI is obliged to cover participants who meet legal requirements and criteria.[3] As part of the welfare state,[4] the SHI is a solidarity-based insurance system,[5] where contributions are paid equally by employer and employee, and employee contributions are based on their income.[6] Regardless of the contribution amount or the duration of membership, insured persons can claim benefits under SGB V. The relevant factor is that the legal requirements are met, and the principle of economic efficiency is observed.[7] Regardless of contribution amount or duration of contribution, all insured persons are eligible for the same catalogue of benefits. The benefits are available as benefits-in-kind, which distinguishes SHI from the reimbursement of private health insurance. The principle of benefits-in-kind plays an important role in the system, as it separates the process of caregiving from the transactions related to payment for services rendered, and requires the care to be appropriate and economical with an eye toward modern standards of care.[8] It is therefore important that digital innovations find their way into the catalogue of benefits so that all insured persons have equal access and a quality, economic care is insured.

2.1.2. *Data protection in healthcare*

Digitization in healthcare depends on the use of sensitive data. Health data fall under the special protection of a complex system of data regulation at several legal levels.

The European General Data Protection Regulation (GDPR) applies to the use of health and care data in Germany. For processing personal-health data, Article 6 and Article 9 of GDPR must be met. According to these provisions, data processing is generally prohibited unless there is explicit consent or a legal basis for it.[9] Legal bases can be found not only in the GDPR directly, but also in national law. For the processing of genetic, biometric and health data, national legislators have the option of enacting their own rules under Article 9 (4) GDPR. Member States, therefore, could enact stronger protections. With health data, for example, Member States can require stricter conditions for processing health data for special purposes, such as research. The German legislature took advantage of the possibilities enabled by the GDPR to enact stricter and supplementary regulations in the German health sector. This affects, for example, genetic data and health-data processed by the SHI.

[2] For current figures and graphs, see www.gkv-spitzenverband.de/service/zahlen_und_grafiken.
[3] Sec. 5-10 SGB V.
[4] Article 20 GG.
[5] Sec. 1 SGB V.
[6] Sec. 3 SGB V.
[7] Sec. 2 SGB V.
[8] W. Rehmann and C. Tillmanns, *E-Health / Digital Health: Rechtshandbuch*, Munich, C. H. Beck, 2022, 69.
[9] If Article 9 (2) of the GDPR applies to processing in the healthcare sector, additional procedural and technical safeguards must be put in place given the sensitivity of the data.

Many provisions concerning data protection in Germany are spread across different areas and bodies of law, such as the Drug Act, the Infection Protection Act, and the Medical Devices Act. This holds true not only at the federal level but also at the state level, where several other data regulations (e.g., in the state hospital laws or cancer registry law) exist because states within Germany also maintain legislative competence in health care. Consequently, data protection in Germany, particularly in healthcare, is fashioned through a patchwork of provisions.

Despite the patchwork, protection is woven into a functional operation. Generally, in the German system, federal law pre-empts state law, and law specifically related to a topic takes precedence over more generally applicable provisions. This allows, for example, special regulations in the SGB V to take precedence over more-general regulations of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG).[10] However, navigating data regulation remains a challenge, even if personal data are only exchanged in Germany (for research purposes, for instance), given many different state data-protection laws in effect, each of which may contain special, specific regulations. The result is a very complex regulatory system.[11] Absent complete European harmonization of data regulation, especially in the healthcare sector, the broad patchwork in Germany persists alongside European law.[12] This creates barriers to care and research.

2.2. *The German Digital Health Strategy*

The German Federal Ministry of Health published a new Digitalization Strategy in March 2023, which has been developed by a participatory process.[13] The development of the strategy required a common national understanding, and the willingness of all stakeholders to participate in implementation endeavours, especially because the new strategy is pursuing ambitious goals. The strategy is intended to help Germany become a pioneer in digitization. The German government has the ambitious goal of finally moving Germany up from the bottom of the international rankings in digitization. When it comes to digitization, especially in the health sector, Germany lags far behind similarly situated nations and healthcare systems.[14] This lag is attributed to conflicts of interest between relevant actors, self-administration, bureaucracy, high technology costs, security concerns, absence of as well as cumbersome regulations, and a lack of technical solutions to remedy interoperability challenges.[15] In light of these perceived stumbling blocks, central topics and core themes of the strategy are new processes in the areas of health and professional care, patient sovereignty, digital competencies, public and provider acceptance, regulatory frameworks, economic efficiency and data management. These diverse topics illustrate the range of variation required for optimal digitization and integration into the existing system.

Efforts to edit the existing system to include and support frameworks that will prove flexible enough to address the integration of future innovations remains the overarching goal, and simultaneous challenge, for health authorities. Indeed, the Ministry needed to develop a strategy that is "future-proof"[16]. The focus of the strategy is on the broader use of health data to improve healthcare and research by further developing already-existing digital applications, implementing new structures into the German healthcare system, and connecting to European and international concepts of data spaces. Despite the nation's experiences during the COVID-19 pandemic that shoved digitization deficits into the spotlight, momentum in the arena appears to have slowed, prompting Minister of Health Karl Lauterbach to undertake responsibilities not

[10] Sec. 1 (2) Sentence 1 BDSG.

[11] Deutscher Ethikrat, Big Data und Gesundheit. Datensouveränität als informationelle Freiheitsgestaltung, Stellungnahme, 2017, 145, in www.ethikrat.org/publikationen.

[12] J. Kühling, *Datenschutz im Gesundheitswesen*, in *Medizinrecht*, vol. 2019, 611-613.

[13] See www.bundesgesundheitsministerium.de/themen/digitalisierung/digitalisierungsstrategie.html.

[14] In the "Bertelsmann Foundation's international comparative study" of 2018, Germany ranked 16th out of 17 countries (www.bertelsmannstiftung.de/de/themen/aktuelle-meldungen/2018/november/digitale-esundheit-deutschland-hinkt-hinterher); Deloitte, Digitalisierung des Gesundheitsmarkts, 2019 (www2.deloitte.com/de/de/pages/life-sciences-and-healthcare/articles/digitalisierung-des-gesundheitsmarktes.html); Sachverständigenrecht Gesundheit & Pflege, Digitalisierung für Gesundheit, 2021 (www.svr-gesundheit.de/gutachten/gutachten-2021).

[15] Fraunhofer, *E-Health in Deutschland*, *Studie zum deutschen Innovationssystem*, No. 12, 2022.

[16] www.bundesgesundheitsministerium.de/themen/digitalisierung/digitalisierungsstrategie.

just as minister of health, but also as a "digitization minister".[17] Digitization in healthcare is a central topic of the current legislative period.

There is a consensus that digitization in Germany needs to move faster, matching the pace of current development and innovation, a pace which to date seems at odds with the rate of detailed integration efforts. While the strategy must inherently consider the complexity of the German healthcare system and data-protection laws, it should not let the complexity stymie progress.

3. *An Overview of the Legislative Pursuit of Digitization in Healthcare*

To ensure that the development of digitization in the healthcare sector in Germany progresses more quickly, the Federal Ministry has adopted several legal measures in recent decades. The following section briefly and chronologically describes the hallmarks of major legislative acts that have exerted a significant impact on the availability of digital technology and services in the public-health insurance system.

3.1. *2003: Initial Steps toward Digitization*

The GKV-Modernisierungsgesetz (GMG) of 2003[18] took initial steps toward digitization by introducing the Electronic Health Card (elektronische Gesundheitskarte - eGK) in January 2006 and the Telematics Infrastructure (TI) a few years later.[19] However, neither venture proved initially successful. The Electronic Health Card serves as proof of eligibility for benefits of the SHI. A microchipped Electronic Health Card contained an insured individual's photograph and personal information, including his or her name, date of birth, address, insurance number and insurance status. Only years later were more functions added to the Electronic Health Card.

The Telematics Infrastructure, the practical significance of which has increased over time, is the network of IT systems that enables links between information sources. In 2005, "Gematik" was founded as the operating company of the Telematics Infrastructure. It is the central platform for digital applications in the German healthcare system.[20] Because of only a partial connection between service providers and the Electronic Health Card's lack of added value, the effect of the law that instituted these innovations was very limited, and digital potential was not maximized. The impact of the unrealized vision and initial setbacks proved consequential, influencing subsequent legislative endeavours.

3.2. *2015/2016: A Digitization Booster*

More than ten years later, legislative action toward digitization in the healthcare sector recommenced with the "E-Health Act" of 2015, which came into force in January 2016.[21] This act initiated relevant developments to the Telematics Infrastructure, the data highway designed to connect all stakeholders in healthcare under a high level of protection. For the first time, the legislature introduced concrete deadlines and sanctions for connecting practices to the Telematics Infrastructure, while also naming specific digital applications. The provision of telemedicine services, such as online video consultations and online radiographic reporting, was encouraged by the new law. Documents like medication plans and provider letters were supposed to be integrated into the Electronic Health Card. Starting in 2018, it was planned to be possible to store emergency medical data on the card at the request of the insured person. Those data include, for example, important information about the blood group, existing vaccination protection or allergies and previous illnesses. The Electronic Health Card is intended to serve as a key that connects patients to the new infrastructure and provides them with easy access to their health data. However, the ambitious goals of the law have not been achieved in practice.

3.3. *2019: A Digital Rush*

A flood of legislation to provide a secure and practical framework for a digital healthcare system began in 2019. The TSVG[22]

[17] www.politico.eu/article/germanys-digital-health-efforts-are-flailing-is-a-lauterbach-strategy-the-ticket.

[18] Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz - GMG), 14 November 2003, in BGBl, 2003, 2190.

[19] Gesetz zur Organisationsstruktur der Telematik im Gesundheitswesen, 22 June 2005, BGB1. I 2005, 1720.

[20] www.gematik.de.

[21] Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz), 21 December 2015, in BGBl, 2015, 2408.

[22] Gesetz für schnellere Termine und bessere Versorgung (Terminservice und Versorgungsgesetz - TSVG), 6 May 2019, BGBl. I 2019, 646.

obliged statutory health insurers to offer an Electronic Patient Record (elektronische Patientenakte - ePA) for insured persons by 2021. Patients should be able to access their treatment data easily, securely, and quickly, using only a smartphone or tablet. In addition, in 2021 the certificate of incapacity for work was supposed to be digitally exchanged between the doctor and the health insurance. Furthermore, the Federal Ministry of Health acquired majority decision-making power in Gematik to implement changes in the Telematics Infrastructure more quickly.

Just a few months later, the next piece of legislation, the Gesetz für mehr Sicherheit in der Arzneimittelversorgung (GSAV),[23] sought to make the drug supply easier and safer. GSAV obliged stakeholders to create the necessary regulations for the use of an Electronic Prescription (eRezept) within seven months after the law came into effect. In addition, prescription drugs could be dispensed by pharmacies after even exclusively-remote treatment.

Soon after, the legislature passed the Digitale-Versorgung-Gesetz (DVG).[24] The ongoing challenges within the Telematics Infrastructure and the patient's changing preferences were the main starting points for the new regulations.[25] The focus was on apps available via prescription, easy use of video consultations and secure access to the healthcare-data network for medical treatments. Prescription Digital Health Applications (Digitale Gesundheitsanwendungen - DiGA)[26] can be used to enhance the treatment of a wide range of illnesses by imparting information, providing context, or guiding patients through exercises. By including them in standard care, the legislator wanted to ensure health and privacy protections, but also to harness the potential of e-Health for the benefit of cost-effective health care.[27]

Moreover, the law made Electronic Patient Records compulsory for hospitals and pharmacies. Pharmacies were required to connect to the necessary digital infrastructure by the end of September 2020 and hospitals by January 2021, with the costs of voluntary connection to be reimbursed. Physicians who remained disconnected would face an increased fee deduction of 2.5%, raised from 1%, starting in March 2020. For midwives and physical therapists as well as nursing and rehabilitation facilities, connection to the Telematics Infrastructure remained voluntary. However, the pressure has been increased to join the digital system, as its success relies on the participation of all system actors. Though the exchange of paper should be overcome, additional premeditated regulations for the Electronic Patient Record were postponed in favour of specifically addressing them in subsequent legislative processes.

3.4. *2020: Focusing on Data Protection*

Less than a year later, in 2020, the Patientendaten-Schutz-Gesetz (PDSG)[28] built upon previous developments, particularly concerning Electronic Patient Records and Prescription Digital Health Applications. The act does not represent a fundamentally-new orientation of the legal concept, but rather ushers in various individual adjustments.[29] It focuses primarily, though not exclusively, on protecting sensitive health data. Every user of the Telematics Infrastructure is responsible for protecting processed patient data. With new and secure apps, insured persons can fill e-prescriptions at a pharmacy of their choice and providers can transfer specialist referrals digitally. Patients were also given the right to have their doctor fill out their electronic patient record. From 2022 on, insured patients can store their vaccination cards, maternity records, children's health booklets and the dental bonus booklet in their Electronic Patient Record, and patients can transfer data to new insurers if changing insurance providers. The record should be user-friendly and offer many different options to the user. The idea is that the patients manage the record themselves, and decide what happens to their data, especially what data are stored, deleted or accessible by others. After much debate,

[23] Gesetz für mehr Sicherheit in der Arzneimittelversorgung (GSAV), 9 September 2019, BGBl. I 2019, 1202.
[24] Digitale-Versorgung-Gesetz (DVG), 9 December 2019, in BGBl, 2019, 2562.
[25] J. Weyd, *Digitalisierung in der Gesetzlichen Krankenversicherung*, in *Medizinrecht*, vol. 38, 2020, 183.
[26] Details under 4.
[27] L. Münkler, *Health-Apps im gesundheitsrechtlichen Regelungsgefüge*, in *Neue Zeitschrift für Sozialrecht*, vol. 2, 2021, 43.
[28] Gesetz zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur (Patientendaten-Schutz-Gesetz - PDSG), 14 October 2020, BGBl. I 2020, 2115.
[29] C. Dochow, *Das Patienten-Datenschutz-Gesetz (Teil 1): Die elektronische Patientenakte und Telematikinfrastruktur*, in *Medizinrecht*, vol. 38, 2020, 979-981.

every person with SHI receives the option to voluntarily make the data stored available to research as a "data donation", starting in 2023. The law strengthened patient sovereignty and patient autonomy, but also raised privacy concerns that led to subsequent improvements during the legislation process.[30]

3.5. *2021: Further development of digital applications*

In 2021, the Digital Supply and Care Modernization Act (DVPMG) was passed[31]. The law aimed at digital support for care, including more opportunities for telemedicine services and modernized networks in healthcare outside of direct medical treatment. Besides the introduction of Digital Care Applications (Digitale Pflegeanwendungen – DiPA) to support people in need of care[32], Prescription Digital Health Applications (DiGAs) were further developed. Data from DiGAs are supposed to be directly transferred to the Electronic Patient Record. Furthermore, data privacy and information security of DiGAs will be strengthened by introducing mandatory certificates for data privacy and information security. The possibility to reimburse DiGAs in an increasing range of fields is growing, as is the access to and range of reimbursable telemedical services. Provisions for updating the Telematics Infrastructure, for example, will allow insured persons and providers to receive digital identities for secure authentication in a video consultation or with DiGAs beginning in 2023.

3.6. *2023 and Beyond: Status and Prospects*

After a slow start in the early 2000s and a peak in 2019, legislative actions toward digitization in healthcare continue to expand and improve the many aspects of a digitized health system,[33] which reflects a consistent review and refinement towards Germany's digital goals. Some acts such as the DVG and the PDSG were specifically aimed at digitization in healthcare, while others, for example the TSVG, address several different innovations.[34] This reflects the experience that societal or system constraints may prevent immediate implementation of digital innovations in their totality, which results in an implementation that takes place over several incremental steps. These include major changes such as the Electronic Health Card and the Electronic Patient Record. For example, since January 2021, insured persons have been able to obtain an Electronic Patient Record, the functions of which are gradually being expanded, from their health insurers. But neither patients nor providers always embrace new care options. Voluntary use may not translate into high demand, as Germany's experience with the Electronic Patient Record reflects. Historically low Electronic Patient Record usage means that newly proposed regulations aiming to establish electronic records as defaults will bring Electronic Patient Records to 80 percent of SHI patients by 2025.[35] (Patients can still opt out if they wish). Both pieces of proposed digital-health legislation in 2023, the Digital Act (Digital-Gesetz – DigiG)[36] and the Health Data Use Act (Gesundheitsdatennutzungsgesetz – GDNG)[37] focus on the support and expansion of the Electronic Patient Record. While the Digital Act aims to simplify and streamline healthcare with digital solutions, the Health Data Use Act seeks to enhance opportunities to responsibly use health data for research.[38] Both new laws are intended to drive the exchange and use of health data and provide targeted support for care. E-prescriptions are anticipated as a mandatory standard as of January 2024. Existing health-care structures are to be better utilized and interconnected.

[30] BfDI (The Federal Commissioner for Data Protection and Information Security) very critical at the time: www.bfdi.bund.de/SharedDocs/Pressemitteilungen/DE/2020/20_BfDI-zu-PDSG.html.

[31] Gesetz zur digitalen Modernisierung von Versorgung und Pflege (Digitale-Versorgung-und-Pflege-Modernisierungs-Gesetz - DVPMG), 3 June 2021, BGBl. 2021 I, 1309.

[32] For more: www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/DiPA/_node.html.

[33] For an overview of milestones, https://gesund.bund.de/digitalisierung-im-esundheitswesen#einleitung.

[34] Acts such as the TSVG are called "Omnisbusgesetz" for this reason.

[35] www.bundesgesundheitsministerium.de/presse/pressemitteilungen/digitalisierungsstrategie-vorgelegt-09-03-2023.

[36] Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz - DigiG), Drucksache No. 435/23 (Gesetzentwurf der Bundesregierung); current consultation status: forwarded to the Bundesrat - not yet discussed (September 2023).

[37] Entwurf eines Gesetzes zur verbesserten Nutzung von Gesundheitsdaten (Gesundheitsdatennutzungsgesetz-GDNG) Drucksache No. 434/23 (Gesetzesentwurf der Bundesregierung); forwarded to the Bundesrat - not yet discussed (September 2023).

[38] www.bundesgesundheitsministerium.de/presse/pressemitteilungen/digitalisierungsstrategie-vorgelegt-09-032023.

Ease in linking data from multiple, different sources should enable greater data utilization. Through these laws, Germany wants to create the preconditions and infrastructure necessary to connect to a European health-data space.

It remains to be seen whether the announced legislative initiatives will resolve the longstanding issues related to implementation. The past has shown that neither the promise of financial incentives nor the threat of sanction has been entirely successful in achieving absolute digitization of the healthcare system nationwide. Nevertheless, regulators are again deploying deadlines and sanctions, and once again stakeholders are raising data protection and practical concerns.[39] Much scepticism about digital innovations remains. Even those willing to engage with new opportunities and offers are discouraged by technical problems that limit digital capabilities. For example, while nearly 100 percent of medical practices and pharmacies are connected to the Telematics Infrastructure, one in two medical practices complain of technical errors at least once a week.[40] As more stakeholders and patients are incorporated into the digital system by growing legal pressure, the system must deliver on its promises in practical terms, particularly in the domain of compulsory SHI. Creating the legal framework is only one part of the complex and long-term digitization process and must be flanked by technical guarantees.

4. *Prescription Digital Health Applications (DiGAs) – an Exercise in Innovation Integration*

The legislative efforts attempt to address the myriad aspects of digitization in its many possible mediums and modes. One digital innovation prompted a new design and structure to be built into the system – the digital health application. Digital health apps attest to the potential of digital technologies in health promotion and reflect the aspirations of system stakeholders to pursue health through technology capable of overcoming existing challenges. To practically leverage the technology quite literally at the fingertips of millions of patients, legislators sought to undertake the integration of health apps as one key component of digitizing the system, seeking to incorporate the prescription and reimbursement of health applications into the offerings of the public insurance system. Doing so required devising an original system, one that enabled insurers to select and reimburse effective health apps from the millions of health and wellness apps populating digital app marketplaces, while simultaneously empowering patients to play active roles in their health management.

The experience of integrating Prescription Digital Health Applications (DiGAs), the health apps and web applications that are made available by healthcare-provider prescription, into the SHI illustrates the influence of the previously-discussed legislative actions, and how they translate into the system. This section highlights DiGAs as a case study, as it sits at the intersection of healthcare delivery, technological innovation, and data protection. The subsequent section details the integration of DiGAs, therein illustrating not only the progress but also the challenges in implementing new digital services in the German healthcare system.

4.1. *Introduction*

The Digital Care Act of 2019 introduced DiGAs to patients in the SHI system. General regulations for DiGAs were established in Book V of the German Social Code.[41] With Sec. 33a SGB V, a new entitlement to benefit was incorporated into law. According to Sec. 33a (2) SGB V, a DiGA is a class I or IIa medical device according to Medical Device Regulation or Medical Device Directive.[42] Class I or IIa medical devices are products that have obtained CE-marking and pose a low risk of potential harm caused by a defect or functional failure of the medical device. DiGAs can support the treatment of a wide variety of conditions, such as migraines, tinnitus, various types of cancer, multiple sclerosis, diabetes, and depression. Some serve to detect or monitor symptoms that

[39] For different perspectives, see www.gkv-spitzenverband.de/gkv_spitzenverband/presse/pressemitteilungen_und_statements/pressemitteilung_1661504.jsp (GKV-Spitzenverband); www.kbv.de/html/1150_65129.php (KBV); www.kzbv.de/digitalisierung-des-gesundheitswesens.1778.de.html (KZBV).

[40] E-health Monitor 2022, available at www.mckinsey.de/news/presse/ehealth-monitor-2022.

[41] Supplemented by Digitale Gesundheitsanwendungen-Verordnung, 8 April 2020, BGBl. I 2020, 768.

[42] DiGA are to be extended to benefit medical devices in risk class 2b, BMG, *Digitalisierungsstrategie für Gesundheit und Pflege*, 2023, 30; Drucksache No. 435/23, 97.

require further investigation. Others promote the health competence of users and enable them to manage their health. Most DiGAs provide direct support for managing illnesses and relieving symptoms. However, software that serves purely to provide knowledge, enable communication, or store information is not considered a health app under the current legal definition.[43] DiGA classification does not include health apps that focus on wellness or fitness and are solely used for primary prevention.[44]

To be reimbursed for DiGA use, a physician's prescription or written proof of a relevant diagnosis is required. The prescription must indicate the name of the DiGA and its pharmaceutical registration number. The patient submits this documentation to the health-insurance provider. After the manufacturer and the SHI fund cross-check the anonymized data, the patient receives an activation code that he or she can enter in the DiGA interface or on the manufacturer's website in order to use the DiGA free of charge.

4.2. *Registry*

The German Federal Institute for Drugs and Medical Devices (Bundesinstitut für Arzneimittel und Medizinprodukte, BfArM) provides an online registry that lists those DiGAs that have successfully passed an assessment for reimbursement.[45] The BfArM plays a central role in concretizing the entitlement to SHI benefits. This contradicts the usual SHI system practice, where the Joint Federal Committee (Gemeinsamer Bundesausschuss, G-BA)[46] is otherwise responsible for such decisions. In contrast to the G-BA, known for long and cumbersome decision-making processes, the BfArM promises faster access to digital innovation. The approval is designed as a fast track and takes a maximum of three months after the complete application of the manufacturer. After that, the manufacturer can enter price negotiations with the National Association of Statutory Health Insurance Funds (GKV-Spitzenverband). Only DiGAs that have been classified for the official list by the BfArM are included in the SHI reimbursement system. Accordingly, this is a positive list with normative character. Such a registry, outside of G-BA review, is new and unusual in the healthcare system.[47] Germany, serving as an international pioneer in the process of establishing DiGAs as standard benefits in the SHI,[48] must nevertheless grapple with constitutional requirements and limitations[49] in their creation of this new path forward.

4.3. *Assessment*

The assessment by the BfArM ensures proof of security, functionality and quality including interoperability, data protection and data security and positive care effects.[50]

The BfArM has been criticized for examining complex data-protection issues as an external body without having to involve a data-protection authority.[51] From August 2024, a certificate in accordance with Article 42 GDPR is required as proof of compliance with data-protection requirements by the manufacturer.[52] Insured persons must be able to rely on the manufacturer's compliance with legal data-protection requirements, careful handling of their data, and implementation of measures to protect confidentiality, availability, and integrity. For this purpose, a regulation (Digitale Gesundheitsanwendungen-Verordnung – DiGAV) specifies and supplements the requirements from the GDPR and other data-protection requirements for the manufacturer's company, for the DiGA itself and for all

[43] V. Lücker, *Medizinprodukterechtliche Rahmenbedingungen für E-Health-Produkte im europäischen Wirtschaftsraum*, in *Bundesgesundheitsblatt*, vol. 3, 2018, 278.
[44] L. Münkler, *Health-Apps im gesundheitsrechtlichen Regulierungsgefüge*, in *Neue Zeitschrift für Sozialrecht*, vol. 2, 2021, 43.
[45] Sec. 139e SGB V; https://diga.bfarm.de/de/verzeichnis.
[46] Sec. 91, 92 SGB V.
[47] Sec. 33a (4) Sentence 2 SGB V.
[48] W. Lauer, W. Löbker, T. Sudhop and K. Broich, *Digitale Gesundheitsanwendungen (DiGA) als innovativer Baustein in der digitalen Gesundheitsversorgung in Deutschland – Informationen, Erfahrungen und Perspektiven*, in *Bundesgesundheitsblatt*, vol. 64, 2021, 1195.
[49] P. Axer, *Verfassungsrechtliche Fragen der Erbringung digitaler Gesundheitsanwendungen nach dem SGB V*, in *Medizinrecht*, vol. 40, 2022, 271.
[50] Sec. 139e (2) SGB V; Digitale Gesundheitsanwendungen-Verordnung-DiGAV; www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/DiGA/_node.html.
[51] See K. Schreiber and B. Gottwald, *Gesundheits-App auf Rezept*, in *Zeitschrift für Datenschutz*, vol. 8, 2020, 390, also for more data privacy issues.
[52] BfArM, Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 138e SGB V, Guidance, Version 3.3, 4 September 2023, 40 for further details.

systems in connection with the DiGA.

A special feature of DiGA assessment is the criterion of positive effects in the supply of healthcare, which includes both clinical benefit and structural and procedural improvements that are relevant to patients.[53] Examples are promoting health literacy, patient sovereignty and better coordination of treatment processes. The proof of positive effect is to be provided by quantitative comparative studies showing that using the DiGA is better than not using it.[54] The requirements for the proof are rather low compared to other SHI services. Furthermore, manufacturers have flexibility in terms of time. They may provide evidence for the benefits of their DiGAs either directly with the application for the fast-track process or generate it during a trial phase that includes temporary reimbursement.[55] All DiGAs in the register are reimbursable by the SHI, regardless of whether the listing is already permanent or initially only provisional. For manufacturers, the BfArM provides a range of support tailored to the requirements (for example, in the form of guidance).[56]

4.4. *Pricing*

DiGA pricing is determined in two stages, when it is included in the directory and one year after the inclusion (Sec. 134 SGB V). After the first year of open pricing, a price for a new DiGA is negotiated between the DiGA-manufacturer and the GKV-Spitzenverband.[57] To this end, the GKV-Spitzenverband has concluded a framework agreement with the top organizations of DiGA-manufacturers on the benchmarks for the agreements on remuneration amounts.[58] An expert committee is responsible for assigning DiGAs to ceiling price groups and for calculating ceiling prices. An arbitration board determined regulations on maximum amounts and thresholds, but there is still plenty of room for manufacturers to achieve high prices for their DiGAs.[59] Maximum amounts have been set for groups of comparable DiGAs, but the maximum amounts are based on the (high) prices of the listed DiGAs. Accordingly, pricing is complicated and can prevent abuse, but does not ensure a fair price from the SHI perspective.[60]

As with innovative drug pricing regulations[61], manufacturers can charge extremely-high prices in the first year of a DiGA's directory inclusion, during which time patients become accustomed to a DiGA. How the price is determined by the manufacturers in the first year and shown in the directory remains non-transparent.[62] Open pricing in the first year also applies to trial DiGAs, which must be reimbursed during this period, even if they have not yet provided evidence of positive-care effects. Limitations are necessary, because the SHI generally does not use the contributions of their insured persons to fund research by manufacturers. It is questionable whether the existing price limits are sufficient.

4.5. *Development*

At the beginning of October 2020, the register went online with the first two DiGAs – the tinnitus app "Kalmeda" and the web application "Velibra" for treatment support in anxiety disorders. From the opening of the application portal to September 2023, 186 applications were submitted.[63] Of these, 146 were requests for provisional admission for testing and 40 were requests for permanent admission. This reflects the increasing interest of manufacturers in provisional admission. The result of the applications is that 49 DiGAs have been added to the list, 16 applications have been negatively assessed and 98 applications have been withdrawn as of

[53] Sec. 139e (2) SGB V; Sec. 8 DiGAV; BfArM, Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 138e SGB V, 92.
[54] For details § 10 DiGAV; BfArM, Das Fast-Track-Verfahren für digitale Gesundheitsanwendungen (DiGA) nach § 138e SGB V, 100.
[55] Sec. 139e (4) SGB V.
[56] https://diga.bfarm.de/de/diga-hersteller.
[57] The negotiations, their preparation, including the consultation documents and minutes of agreement on the amount of remuneration, are confidential. Sec. 134 (1) Sentence 5 SGB V.
[58] Rahmenvereinbarung nach Sec. 134 Absatz 4 und 5 SGB V, 16 December 2021, at www.gkv-spitzenverband.de/krankenversicherung/digitalisierung/kv_diga/diga.jsp.
[59] For more details, see www.gkv-spitzenverband.de/gkv_spitzenverband/presse/fokus/fokus_diga.jsp.
[60] For the different perspectives, T. Severin, Viel Konfliktstoff bei Gesundheits-Apps, in G+G, vol. 3, 2022, www.gg-digital.de/2022/03/viel-konfliktstoff-bei-gesundheits-apps/index.html.
[61] Sec. 35a SGB V.
[62] S. Stoff-Ahnis, *Digitale Gesundheitsanwendungen – Das erste Jahr aus Sicht der Gesetzlichen Krankenversicherung*, in *Medizinrecht*, vol. 40, 2022, 287.
[63] BfArM, 20 September 2023, www.bfarm.de/DE/Medizinprodukte/Aufgaben/DiGA-und-DiPA/DiGA/_node.html.

September 2023. Seventeen applications are currently being processed, and six DiGAs were removed from the list. For data-protection reasons, the BfArM cannot provide information on application details, such as which manufacturers have submitted applications or to which DiGA they refer. Hence, detailed information on unsuccessful applications is not available. Potential bases for failure include, for example, deficiencies in data protection and information security, inability to demonstrate positive effects on the supply of healthcare, or the fact that the studies presented did not satisfy the principles of evidence-based medicine.[64] With time and with each application, manufacturers continue to gain experience and can better meet standards.

4.6. *Evaluation and Perspective*

In its first and second reports (September 2020 to September 2022), the GKV-Spitzenverband took stock of the uptake and development of care with DiGAs.[65] Both reports criticize the lax quality control and the high price in relation to the proven benefits. Even the maximum amounts that have been in force since October 2022 do not significantly limit the very high price level.[66] This contradicts the efficiency principle in the SHI system. According to the statement of the GKV-Spitzenverband, the relatively-low eligibility requirements for DiGAs are also inconsistent with other SHI benefits. Health insurers must provide their insured with DiGAs for which the medical benefit has not been proven and it is unclear whether and to what extent the DiGAs can help. In addition, the practice of the statutory health insurers in approving digital health applications is inconsistent, including the intensity of the review conducted. It is also not transparent whether and to what extent a patient uses the DiGA. However, this aspect should be considered when setting the price for the DiGA, as it is not just about downloads.

There is a consensus that DiGAs can improve healthcare, particularly complementing and supporting existing services, but the law needs to be amended. The planned Digital Act (DigiG) is intended to address this demand.[67] The proposed law requires the GKV-Spitzenverband to issue a guideline with uniform requirements for the approval process. The guideline must specify the scope of the examination and the type of proof of a medical indication as a prerequisite for approval. An exclusion of benefits is provided for products of DiGAs that are only intended for use with certain medical aids or medicines. Based on prior experience, the law will also clarify that it is impermissible for a DiGA to be deliberately created and designed as a result of agreements between various manufacturers that would make the application only suitable for accompanying a therapy with a specific drug, medicinal product, or medical device, thereby rendering the app's use with other suitable medical aids or medicines is impossible. This also applies to other agreements or concerted practices by manufacturers. The clarification is intended to safeguard the insured's freedom of choice and physicians' freedom to select therapies. It is also important to find the balance between proof of benefit and openness to innovation. The evolution of the benefit and its impact will continue to be examined using data on care-delivery patterns. Pending legislation, like the DigiG, underscores that it remains to be seen whether and to what extent DiGAs can be integrated and established in the growing digital-healthcare structure.

5. *Looking Ahead – Prospective Considerations*

Leading the historically complex German healthcare system into a digital age is a long, extensive process. The influx of legislation on digitization in the healthcare sector observed over the last decade is far from final, and stakeholders can anticipate more action as the system continues to build the frameworks that best leverage digital technologies' health benefits. Indeed, the coalition government

[64] W. Lauer, W. Löbker and B. Höfgen, *Digitale Gesundheitsanwendungen (DiGA): Bewertung der Erstattungsfähigkeit mittels DiGA-Fast-Track-Verfahrens im Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM)*, in *Bundesgesundheitsblatt*, vol. 64, 2021, 1238 for a differentiated evaluation.

[65] www.gkv-spitzenverband.de/gkv_spitzenverband/presse/fokus/fokus_diga.jsp.

[66] About 600 to 900 Euro during the free pricing period in the first year; average price after one year about 215 Euro (DiGA-Bericht des GKV-Spitzenverbands, Berichtszeitraum: 1 September 2020 - 30 September 2022, in www.gkv-spitzenverband.de/krankenversicherung/digitalisierung/kv_diga/diga.jsp.

[67] Entwurf eines Gesetzes zur Beschleunigung der Digitalisierung des Gesundheitswesens (Digital-Gesetz-DigiG), Drucksache No. 435/23, 98-99.

agreed on the digitization of healthcare as a shared priority,[68] and new digital laws are on their way. In addition to measures contained in DigiG and GDNG, proposed legislation includes action such as a messenger service for communication between care providers, and at least 300 research projects carried out or initiated using data from a research data center.[69]

With a basic infrastructure established, the system is entering a phase where it must more earnestly consider macro-level questions, beyond legal and technological aspects, related to the digitization process. Societal considerations about digital services and their support outside the healthcare sector must be considered, and that (social) factors external to the healthcare sector have a profound impact on digitization's success should be recognized. The process of digitalization has moved beyond theoretical options to binding practical steps toward nationwide digital coverage. Each participant in the healthcare system has its part to play, with the quality of patient care as the common goal that can be realized by using health data to a much greater extent. The more extensive the participation and the more seamless the system, the more successful digitization will be.

The exercise in DiGA incorporation should remind stakeholders of this in the progress toward flexible digital integration. DiGAs were meant to enhance patient voice, embodying, for example, patient-relevant components in the reimbursement considerations.[70] However, surveys post-implementation revealed preliminary provider reluctance toward DiGA prescription providing, citing lack of evidence and patient and provider education as some of the many reasons for their reluctance.[71]

Following innovation introduction, stakeholders should channel efforts into supporting uptake and integration, ensuring proficient usage of these tools, through actions such as continuing education for providers,[72] and enhancing patient digital literacy.[73] Evaluation of digital integrations will also serve as an instrumental tool in the evolution of digital products and services in the SHI. Looking ahead, reforms should make the system flexible enough to incorporate changes with ease and, ultimately, deliver optimal healthcare to all.

6. *Conclusion*

The potential of digitization in healthcare has not yet been fully realized in Germany, but important steps have been taken. This paper has illustrated how necessary legal frameworks have been implemented in the context of the existing system and are constantly being improved. Regulators must reckon with their role as system influencers, both at present and in the future. They must grapple with and balance inherent and frequently-conflicting interests in the pursuit of digitization. By setting the standards for digitally-enhanced healthcare, they necessarily shape innovation as well, influencing how high or low a standard must be for an innovator to become a player in the healthcare system, and accordingly for a patient to reap the benefits of digital innovation.

[68] Koalitionsvertrag 2021-2025, Zwischen der Sozialdemokratischen Partei Deutschlands (SPD), Bündnis 90, Die Grünen und den Freien Demokraten (FDP), *Mehr Fortschritt Wagen*, in *www.spd.de/fileadmin/Dokumente/Koalitionsvertrag/Koalitionsvertrag_2021-2025.pdf,* 83.

[69] For more, www.bundesgesundheitsministerium.de/presse/pressemitteilungen/digitalisierungsstrategie-vorgelegt-09-03-2023.html.

[70] Federal Institute for Drugs and Medical Devices, The Fast-Track Process for Digital Health Applications (DiGA) according to Section 139e SGB V. A Guide for Manufacturers, Service Providers and Users, Bonn, 2020, 77 (available at www.bfarm.de/SharedDocs/Downloads/EN/MedicalDevices/DiGA_Guide.pdf;jsessionid=437C9A1406E15C4B8D610B488FFC94D8.2_cid329?__blob=publicationFile&v=2).

[71] J. Wangler and M. Jansky, *Welche Potenziale und Mehrwerte bieten DiGA für die hausärztliche Versorgung? Ergebnisse einer Befragung von Hausärzt*innen in Deutschland [What potential and added value do DiGA offer for primary care? Results of a survey of general practitioners in Germany],* in *Bundesgesundheitsblatt Gesundheitsforschung Gesundheitsschutz*, vol. 65, No. 12, 2022, 1334-1343; M. Radić, I. Donner, M. Waack, C. Brinkmann, L. Stein and D. Radić, *Digitale Gesundheitsanwendungen: Die Akzeptanz steigern*, in *Dtsch Arztebl*, vol. 118, No. 6, 2021, 286-92.

[72] S. Sauermann, J. Herzberg, S. Burkert and S. Habetha, *DiGA - A Chance for the German Healthcare System*, *Journal of European CME*, vol. 11, No. 1, 2021, 2014047.

[73] Y. Goldwasser, W.J. Gordon, J.B. Brönneke and A.D. Stern, *On The Brink of a Digital Health Care Transformation: What Germany Can Learn From The United States*, Health Affairs Blog, 2021, in www.healthaffairs.org/content/forefront/brink-digital-health-care-transformation-germany-can-learn-united-states.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 233-241
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 18

*e-Healthcare in Hungary With the Help of ICT Tools**

Balázs Szabó
(Assistant professor, University of Miskolc, Faculty of Law, State Sciences Institutiones, Department of Public Administration Law)

ABSTRACT In addition to the smartphone applications, some specialized administrative bodies of the public administration have additional opportunities to facilitate the activities of the authorities. One of the important technical and development tools of the 21th century, is the big variety of drones, which were originally developed for military purposes. The another most important info-communication tools (hereinafter: ICT) are the smarth-phones. Undoubtedly, these equipments can be apostrophized as probably the most popular technical tools, based on the fact that in addition to their ever-expanding uses, they also provide excellent help for leisure activities and outdoor photo/video documentation. In addition, we can find their application in more and more fields of our Hungarian public administration system. In recent years, the use of smartphones and applications on them, has been successfully introduced in more and more administrative areas, which makes the work of the authorities more efficient and faster, which in many cases can lead to the saving of human lives too. After (?!) the Corona virus pandemic, I have no doubt about, that the health care, and the e-solutions, developements helped a lot till nowadays, and it will be just more important in the next years as well. I will highlighted some of the good practices that I consider to be most important and may give some positive expressions to implement them in other fields.

1. *Introduction*

The development of healthcare is one of the most important interests of society as a whole and one of the sectoral areas of greatest interest. In the life of a modern state, the service provider must be as efficient as possible and of the highest quality. This is especially true for the health sector, where citizens' health and possibly their lives are at stake. That is why the current Hungarian government must also do everything to be able to provide the most modern equipment for healthcare institutions.[1]

In this article, I tried to introduce the most important developements from the recent years, which were originated by the public administration developement programs of Hungary, especially focussing on the „smart-solutions". These developements, which are basically using and need smart phones are the best and necessary answers by the state for the new challgenges. Thanks to the covid-19 pandemic and the many official actions caused by it, the world and thus Hungary has learned that it is advisable to use as widely as possible the smart devices that are present in the largest number of citizens, which are smartphones.

Digital health and care cover the tools and services that use information and communication technologies to improve prevention, diagnosis, treatment, monitoring of health-related issues and as well as monitor and manage the interaction of health and lifestyle, such as artificial intelligence, blockchain, the interconnection of devices (IoT) or the 5G network. Innovative digital healthcare and care can improve the quality of care and access to care, as well as increase the overall efficiency of the healthcare sector or reduce administrative burdens. The topic is extremely difficult, as new projects, participants, or initiatives that "change everything" appear every day. In the following, I would like to briefly present the Hungarian developments.

1.1. *Developments in Hungary*

In connection with the present article, I did not of course wish to present the entire vertical of healthcare developments in Hungary, but specifically tried to present the topic of electronic solutions, software, and applications. In recent years, of course, many organizational changes and developments have taken place, as well as in the field of the development of applied medical technology devices. However, I do not want to address them in this study, not least because the series of organizational transformations does not

* Article submitted to double-blind peer review.
[1] See more about this: Z. Árva, *The role of state bodies in health administration*, in A. Bencsik (ed.), *Public administrative legal knowledge: Study material for healthcare professionals - with special regard to the organization and administration of healthcare*, Budapest, Hungary, Health Registration and Training Center (ENKK), (2016), 18, 55-72.

seem to have been completed yet. In my opinion - and this can also be inferred from the many "signs" that point to this - in the coming period, private health care providers may gain a greater role in Hungarian health care through one or another regulation. In my current topic, however, I am trying to present the electronic public administration developments of state health care providers.

Nowadays, we can say that in addition to the acquisition of devices for domestic medicine, there is also a need for the technical and technological development of health administration. Thanks to the EU subsidies, improvements have also been made in this area in the past period. Among these, the new, *Unified Healthcare Electronic Space* (hereinafter: EESZT) stands out. As part of the solution introduced on November 1th, 2017, it is possible to record the data on medical services, prescriptions, referrals, laboratory tests and other findings in a national online network. The most important purpose and practical benefit of this is that, through the system, this information becomes available to all doctors and pharmacists treating the given client/patient. We can see this as a new digital – and perhaps even more important – unified information source, to which approximately 10,000 healthcare providers have joined.[2] The goal of the program is that by now all institutions and persons providing services in the field of health care will be connected to the Unified Health Care Space.[3]

It is important to emphasize that this health information can only be seen by the patient's general practitioner and treating doctor in the system, so - as a general rule - we do not have to worry about our sensitive health data falling into the hands of unauthorized persons. The system includes the following important service elements.

- *eHealth history;*
- *eRecipe;*
- *eReferral;*
- *Digital Image Transmission;*
- *eProfile;*
- *Trunk publication;*
- *Use of Health Service Space for health care providers*.[4]

The *eHealth History* essentially enables the central storage and retrieval of medical documents generated in connection with individual care events. This may be important when a later disease appears or before surgical intervention. It should be added that within this function, the case history will only store the care documentation, additional documents created during the care will be preserved and stored in other units of the EESZT.

Clients are assisted by the Resident Portal, where everyone can find a list of their care events (in the event catalogue) and view their e-disease history documents created during their care (by clicking on the case history menu item).

The *e-Recipe* is one of the new system's most well-known and perhaps most used modules. Essentially, we already receive an e-prescription, even if it is traditionally printed on paper since the doctor who writes the prescription can also see in the system whether the patient has taken the medication after the prescription has been issued. Accordingly, pharmacies also have the right to see what medicines were previously prescribed to the given patient.[5]

To connect to the EESZT, a web service interface may also be necessary in the case of information systems on the prescriber side (general practitioner, specialist practice, hospital, etc.) and pharmacy information systems. As an additional function, it can be mentioned that a web application is also available for doctors, with which they can view the patient's medication.

The available functions that the system provides to the attending physician are the following services:[6]

- writing medicine prescriptions;
- writing a recurring prescription (ordering a three-month quantity of medication);
- yourself, or withdrawal (logical deletion) of drug prescriptions prescribed by the substituted doctor;
- querying the summary list of drug prescriptions based on Social Security

[2] This is how we consider the general practitioner, the pharmacy, as well as state clinics and hospitals. Private doctors, private hospitals, dentists and ambulances are scheduled to be connected to the system in November 2018.

[3] According to the statement made by minister commissioner Gergely BARTUS on Kossuth Rádió Napközben program on 24 April 2018.

[4] Source: https://e-egeszsegugy.gov.hu/web/eeszt-information-portal/agazati-portal-es-modulok.

[5] Source: https://e-egeszsegugy.gov.hu/web/eeszt-information-portal/e-recept.

[6] Source: https://e-egeszsegugy.gov.hu/web/eeszt-information-portal/e-recept.

Number;
- querying certain drug prescriptions.

One of the fundamental aspects of the introduction of the e-Health system is that we do not cause a break in the currently existing processes, thereby not making the lives of patients more difficult[7]. Thus, it will be possible to order paper-based prescriptions in the future, and handwritten prescriptions (hereinafter: prescriptions) will also remain valid. At the same time, the system creates an opportunity to use modern solutions by providing paper-based prescriptions with Social Security numbers - which, when redeemed at the pharmacy, are entered into the EESZT and searchable in the same way as prescriptions originally ordered electronically - a completely paperless procedure is possible too.

The essence of *eReferral* is to modernize and simplify the previously introduced rules[8]. The eReferral module of the EESZT creates the previously missing data transmission channel between the IT system of the doctor issuing the referral and the doctor performing the examination, thus ensuring the reliable and safe transmission of patients' health data, which is the basic objective of all public administration IT development. During care, the information provided by the referring physician (e.g. preliminary examinations, findings, or current complaints) must be clear to the examining physician. To this end, transmission using electronic means can eliminate the difficulties and risks associated with previous paper-based referrals.[9]

A significant advantage of eReferral is that it created an opportunity for the referring physician to prepare the patient's referrals in a standardized way - even by creating their templates - during which the rules of the referral are checked, and it may be important that the patient's other needs can be taken into account when preparing the referral, their content and time. The referrals sent by the referring doctor are stored in the EESZT and become available to all doctors with authorization and specialist knowledge of the care institution they wish to use. As a result, care can be planned even before the patient arrives, and patient data related to the referral is available in a reliable form and content when the patient logs in. This will result in the attending physician being able to start his diagnostic and therapeutic activities faster and more thoroughly. The fact of the use of the referral is also recorded in the e-referral module, and the referring physician and the patient can receive a notification via the EESZT about the completion of the findings of the services used based on the referral if they so request. During the operation of the system, it is also possible for not only doctors, but also patients to view their referrals through the public portal, and - due to the synchronization of the system with the client portal - it is possible to request notification to our client portal storage about the completion of new referrals.[10]

It is important that because of extraordinary situations (e.g. emergency referrals on the night shift, when it is not possible to record data), the current paper referral option will still be maintained.

Within the framework of the *Digital Image Transmission* function, it is possible to transmit images created and stored by devices of various manufacturers to other healthcare institutions and service providers[11]. Thanks to the rapid development of technology, digital imaging is also appearing in specialist areas where recordings were often not recorded before (e.g. histology, gastroenterology, ECG, EEG). At the same time, digital technology creates the opportunity to quickly and safely transmit digital images between different institutions by applying the standards accepted so far and by exploiting the possibilities of the Internet, thereby increasing the efficiency and safety of patient care. In essence, this can mean cost-effective copying and forwarding, moving images without moving them from

[7] See more in M.Asbóth, M.Fazekas and J.Koncz, *Health Law and Administration*, Budapest, ELTE EÖTVÖS Publisher, 2020.

[8] The essence of this is that it is possible for anyone to use a significant part of the health services based on a doctor's referral. Until now, during the referral, the initiating physicians could only prepare the referral on paper and record the history, possible requests, and findings related to the requested care. In recent years, health care providers have had to accurately record more and more data on these papers, so the IT systems of specialist clinics and hospitals are already prepared to handle the content of referrals electronically.

[9] Source: https://e-egeszsegugy.gov.hu/web/eeszt-information-portal/beutaló.

[10] B. Szabó, *The technical and technological development of the Hungarian public administration in the XXI. in the first two decades of the century*, PhD dissertation, University of Miskolc, Ferenc Deák Doctoral School of Science and Law, 2020, 206-207.

[11] Source: https://e-egeszsegugy.gov.hu/web/eeszt-information-portal/digitalis-keptovabbitasi-es-tavkonzilium.

their original location.[12]

The EESZT offers three different functions to achieve the above goals. First of all, the sharing of the digital image material for healthcare providers joining the EESZT, during which the participants record the list of images created by them in a central database, which can be viewed and downloaded by other providers if necessary.

The second function of the system is a digital image-sending technology, which is a special e-mail system developed for image transmission, without significant size limitations. Its primary areas of application arise when images quickly forwarded that have not yet been shared in the central system (e.g. forwarded by the patient after primary examinations have been completed).

The third function is remote consultation, which also requires online expertise, through which the attending physician can request professional help from other medical colleagues in complicated cases[13]. I consider that this also clearly increases the efficiency and quality of patient care, complying with and complying with data protection rules to protect patient data.

As a module, *eProfil* is designed to ensure that the most characteristic health summary data for patients, their health profile, can be accurately and continuously recorded. The information stored here – in contrast to several modules of the EESZT – is not data on patients' health events, but a health summary (reports) specific to the patient.

It can be stated that the data managed in the eProfile typically do not, or rarely, change and are characteristic of the patient's health status in the long term. This includes data on allergies, drug sensitivities, implants, chronic diseases, participation in care, established diseases, changes, and current medication. Registration in the eProfile can be done by the attending physician and general practitioner, but at the same time, due to the right of self-determination of the person provided, this can also be prohibited.

The *main publication*, as a module, "ensures, as a single service, the publication for the matching systems of the institutions responsible for the code tables, code bases and registers used by several actors, as well as accessibility for the actors who use them, separating the roles and processes of the data owner and the user. The module handles public, public-purpose and technical master data."[14] As a result, the employees of the various healthcare institutions can see the source of the data and documents included in the system. The use of the EESZT for healthcare providers as a module presents the connection process in detail. Within this framework, the system provides the necessary forms, which must be attached through the system. The assembled system sends the confirmation after the documents have been posted, and then the technical implementation of the connection to the system begins[15].

In my opinion, this unified healthcare system can be said to be a development milestone, but at the same time, its introduction was well overdue on the part of the state. It is not up to me to investigate what could have been behind this, but I think it can be clearly stated that the technological conditions in the world and thus also in our country - I mean a reliable, stable Internet connection, a suitable computer network, servers and software - were already available before. Accordingly, the introduction was not an undivided success, which could have been due to a number of reasons. On the one hand, we can talk about a kind of mistrust of digital solutions, and on the other hand, concerns about the Hungarian healthcare network. Both are serious handicaps on their own, but together they are particularly harmful. This was also contributed to by a so-called internal ``resistance'' on the part of the healthcare workers, the main reason behind which, in my opinion, was that they saw it as a new task in an era where they were mostly waiting for an appropriate wage arrangement rather than new types of tasks. The Hungarian state may have managed to resolve this since then, but concerns about digital solutions still exist, not only in healthcare, but also in relation to many public administration services.

[12] B. Szabó, *The technical and technological development of the Hungarian public administration in the XXI. in the first two decades of the century*, 208.

[13] As a personal opinion, I would like to note that the role of this remote council is greatly appreciated in today's severe "doctor shortage".

[14] Source: https://e-egeszsegugy.gov.hu/web/eeszt-informacios-portal/torzspublikacio.

[15] B. Szabó, *The technical and technological development of the Hungarian public administration in the XXI. in the first two decades of the century*, 210.

2. *Smart solutions or the role of mobile applications in healthcare*

Among the healthcare developments, mobile applications, which are gaining in popularity based on download data and user feedback[16], deserve special mention, of which I would like to present the most important ones. In my opinion, the previously expressed concerns and objections to digital solutions have been reduced with useful, life-like and easy-to-use smart phone applications, the usability of which was specifically proven and strengthened by the covid pandemic. In my opinion, if a small positive element can be singled out from the pandemic and its effects, then in the case of Hungary, it is definitely the fact that almost overnight the mobile applications for health purposes, which I would like to briefly present now.

2.1. *Élementő app (Lifesaving app)*[17]

The application's services[18] provide the opportunity to enter important data (e.g.: known illness, treatment, drug sensitivity, etc.) in advance so that they are displayed at the same time as the emergency call at the rescue controllers at the press of a button. The rescuers will not only see the location (exact geographical position) of the person in trouble but also the battery level of the phone, which can be useful information in case the device is drained. In many cases, the quick arrival of the ambulances also depends on whether it is possible to know the exact geographical location of the patient. With the help of the application, the user can immediately contact the rescue controllers of the National Ambulance Service. Simultaneously, the application sends a message to the rescue control centre with the user's data, including his location. The positioning function also shows us our position measured by GPS, the nearest defibrillator, hospital, clinic or pharmacy. The application indicates what you are looking for and can quickly navigate us there. Another important function is the lifesaving guide. Providing first aid until the ambulance arrives increases the patient's chances of survival and recovery. The ÉlétMentő application provides help and supports with its interactive guide, which looks at the most important steps by topic so that life-saving can begin professionally.

2.2. *Szív City (Health City)*[19]

The application was created for a similar purpose, i.e. to help save lives. Szív City is a virtual community whose volunteer members are ready to save public victims of circulatory arrest (sudden cardiac arrest). By downloading the Szív City app and registering, they agree that if someone near them has a heart attack, they will rush to the scene when the National Ambulance Service is alerted, and start reviving them before the ambulance arrives.[20]

I don't think the COVID epidemic needs to be introduced to many people. In March 2020, it almost burst into our lives like a stroke of fate. We didn't know what was happening, only that there was trouble and that a pandemic was sweeping the world. The first months were very difficult, as most of the states were not prepared for everything. Suddenly, it was necessary to quickly switch to online education, carry out numerous administrative tasks and comply with quite a few restrictive measures, such as continuous disinfection and the use of masks. Fortunately, we have since learned that the vaccines that have been developed are a kind of solution to this pandemic. However, the mobile applications created during the epidemic also provided great help for this, which serve the interests of both the authorities (health, law enforcement, etc.) and the population in the field of information, contact research and administration. Applications related to this covid-19 epidemic include the *Virusradar* and the *Home Quarantine application.*

2.3. *Virusradar*

This is a mobile application developed based on the best international examples for protection against the coronavirus. This application, like similar solutions around the world, has become one of the most important digital tools for protection against the corona virus.

With the help of the application, contact with proven infected people can be

[16] Source: https://minap.hu/cikk/nepszeru-mentos-applikacio.
[17] B. Szabo, *The technical and technological development of the Hungarian public administration in the XXI. in the first two decades of the century*, 216.
[18] Source: https://www.mentok.hu/ha-baj-van/eletmento-app/funkciok/.
[19] B. Szabo, *The technical and technological development of the Hungarian public administration in the XXI. in the first two decades of the century*, 217.
[20] Source: http://szivcity.hu.

investigated by measuring the distance of mobile devices using Bluetooth. VírusRadar made the work of epidemiologists easier in contact tracing. The app communicates with other users via Bluetooth and exchanges encrypted, anonymized data about the distance of nearby devices if they have been within a dangerous distance in the last 14 days. If a user becomes infected, the user may share the app's data with epidemiologists. Professionals can ask the infected person using the information to share the data, thereby notifying people who were in close contact with the infected person.

These types of mobile applications have been developed and introduced worldwide in a short period of time with the same goal of notifying users that a person with the corona virus is nearby. Of course - perhaps rightly so - data protection concerns were raised worldwide, but it could have been one of the most effective means of spreading the virus. The use of the conditional mode is no accident, since in my opinion this application can be really effective if everyone uses it. However, this can only be achieved by making it mandatory. Few countries dared to introduce such at the very beginning, but the ones that did, Australia is an excellent example of this, the number of illnesses there has significantly decreased. It is interesting that from the very beginning, Australia made it mandatory for all adult citizens to download the "Virus Radar" application there, with which they were able to manage contact tracing in case of infection with record speed. However, the infection could still happen despite these efforts, which another application tried to help on the part of the authorities.

2.4. *Home quarantine*

This application made it easier for people to request this type of control method when they were quarantined. In this way, making the work of others easier, in this case, the work of the police did not have to pay their respects to the person currently in quarantine, but with the help of the application, when he downloaded and registered himself, he was able to use a photo every single day to prove that he had complied with all regulations he does not leave the house and takes the quarantine rules seriously. In doing so, the persons under control must complete the following steps for the authorities. Start the application and log-in. After that, you need to tap on the "Start Remote Control" button. Then the application will start the camera, during which you have to look into the front camera of the phone and follow the instructions on the screen, then wait until the message "Remote control successful" appears on the phone screen. When taking the photo, it is also important to make sure that only the person under control appears in the photo, and that no other person is visible in the photo.[21]

If in the past I have mentioned citizen mistrust, then this point of concern must be addressed in this application as well. The essence of the program is that it helps the work of the authorities by allowing people who are quarantined due to the infection to have a place to register at any point of the day. In doing so, the authority can oblige the citizen to prove whether or not she is really staying in the place designated for the quarantine period, even with the camera turned on. Many consider this to be an unjustified interference in the human private sphere, and in my opinion, perhaps for an obvious reason. At the same time, it is an indisputable fact that the purpose of this is also to prevent and reduce the spread of the epidemic as soon as possible.

2.5. *EESZT App*[22]

The previously mentioned *EESZT* system was able to expand with a new important element after the outbreak of the coronavirus epidemic. The developed *EESZT mobile application*, which is an important new element enables the use of a downloadable electronic vaccination certificate. With the application, we got relief in that if we have already received the vaccination, we do not have to wait to receive our protection certificate in the form of a card, but if this application is downloaded, they can easily and quickly check our protection/vaccination with the help of a QR code in places where entry is only possible with a protection card. Such as the interior of cinemas, theatres and restaurants. So if the person has already received his vaccination, he can download the application and not have to wait days or even weeks for the little card to be sent out because

[21] Source*:* https://hazikaranten.hu/hogyan-mukodik-az-applikacio.

[22] B. Szabo, *The technical and technological development of the Hungarian public administration in the XXI. in the first two decades of the century*, 219.

the application is connected to the EESZT IT system used by vaccinators, so they are already registered there.

Earlier, with the main EESZT system, I already explained what problems and concerns arose in relation to the system, both internally - on the part of health workers - and on the part of citizens. In my opinion, this was improved by the smartphone application of the system, which made e-Health more lifelike and usable, and actually more visible and tangible for citizens. With the help of this, this application really helped, supported and made their lives easier for the users, for example, in connection with the portability of previously issued paper-based protection certificates in digital form with the help of this software.

2.6. *AIPDerm*

The *AIPDerm* application can represent a new level of digitization and modern solutions. During the AIPDerm teledermatology service, we scan our suspected skin disease with the help of our smartphone camera. If we have a dermatological problem, we simply take a photo and upload the picture of it to the AIPDerm application via smartphone or computer. Here, in addition to uploading our data and high-quality photos, it is also necessary to enter the experienced symptoms. Artificial intelligence (AI) supports the doctor in dermatological examination, which can be used remotely or even from home. Based on the mobile phone photos and the patient's message, the MI combs through its huge database, containing around two million photos, in seconds. The machine recognizes 700 diseases, which is 95 percent of skin problems, and according to AIP Labs, it has no equal in the world. The machine thus selects the three or five diseases it considers most likely[23]. After that, the attending physician determines the final diagnosis and treatment with the help of Artificial Intelligence, can prescribe the use of over-the-counter medicinal products or a prescription, and in the case of a serious illness, recommends that you visit a specialist in person. The prescription can be redeemed at any pharmacy through the EESZT. Finally, a monitoring system helps to follow the patient's recovery and prevent future illnesses.[24]

3. *Usability of drones in 21st-century healthcare*

In the following, I examined the applicability of a tool that is currently only in an experimental phase on the map of the digitalization of Hungarian healthcare[25]. In my opinion, in addition to smartphone applications, some specialized administrative bodies of the Hungarian public administration have additional opportunities to facilitate the activities of the authorities with other excellent tools. The XXI. One of the important technical and development tools of the 20th century is the range of drones originally developed for military-technical purposes[26]. Drones can undoubtedly be considered one of the most popular technical devices, based on the fact that, in addition to their ever-widening range of uses, they also provide excellent assistance for leisure activities and outdoor photo/video documentation.

I am aware that there are dangers in the use of drones, which I do not want to go into in detail in this study, because the article deals with the modernization of healthcare. In the course of my research, I considered drones as a tool, the use of which in certain administrative areas can greatly contribute to making the work of the given authority more efficient and effective. In addition to the mentioned mobile application, the use of drones may be another important element of healthcare administration in the future.

The project that Alec Momont first developed[27], as a prototype of the first aid drone, could be used for a rather special, but at the same time useful for society as a whole. The essence of this is that the drone is equipped with a defibrillator, which can be deployed in areas that cannot be reached in minutes with other vehicles. The developed

[23] https://hvg.hu/360/202306__tavgyogyitas_idosfelugyelet__borrakszures__noverhivo_aplafonon__orvosi_gepesites.

[24] *www.aipderm.hu*

[25] See more in M.Asbóth, M.Fazekas and J.Koncz, *Health Law and Administration*, *op cit.*

[26] Unmanned Aerial Vehicle, UAV, or Remotely Piloted (Aerial) Vehicle, RPV, or drone (the meaning of the English word drone testicle (beehive)), which in the beginning is an aircraft primarily used for military tasks, which has some kind of self-control or remote control (most often a combination of the two), so there is no need for a pilot on board.

[27] Source: https://index.hu/tech/2014/10/30/eletet_menthet_a_defibrillator_dron/

device has quite serious features, as it has a load capacity of approximately four kilograms and can cover an area of twelve square kilometres with approx. it reaches in one minute, thereby increasing the patient's chances of survival to an unprecedented extent compared to the traditional, much slower means of delivery. The question arises here, how should the device be used, how can it save lives? Due to the development of healthcare-technology,[28] it is also possible to carry out lifesaving in real-time, remotely, following the instructions given by a specialist. Documented life-saving successes are also associated with the technology. A case in the USA is worth mentioning, during which local disaster management and fire department staff rescued two young people caught in a flood. With the help of a drone managed by the fire department, it was possible to survey the terrain, then use the device to drop rope and life jackets, and finally carry out a successful rescue.[29]

Thanks to the results of a Swiss experiment (which lasted from March 2017 to October 2017), to process laboratory samples faster, drones are also used to transport not-too-heavy samples between different healthcare institutions[30]. Their delivery does not require too much strength and energy, but speed is necessary, in many cases, lives can depend on how quickly a result arrives. This is also why we can consider the medical use of drones as a rather innovative solution, which can be used to avoid the loss of time caused by urban traffic and especially traffic jams. In addition to samples, it is of course also possible to deliver blood, medicines or other materials related to health care over long distances.[31]

For those who live in a less urbanized area, getting to a doctor or medicine can be difficult. This is also why the continuous development and testing of drones in this area is important, as their use can improve the quality and efficiency of healthcare services, as well as their perception by society, realizing the objectives of the concept of the Good State.

Disaster management staff have already deployed drones in Hungary as well. The Baranya County Special Rescuers tried to find a man missing in a mine with the help of a drone. In addition to the manpower search, they used the possibilities offered by the drone and scanned the area of the reeds of the lake from a height of a few meters from the shore, which was monitored by the disaster prevention staff standing on the shore through a screen.[32]

In addition to the detection of weevils, the other area where drones are being used on an experimental basis is in connection with the transport of small medical devices, medicines, and possibly blood. However, there are still countless obstacles to this, which have not yet been solved creditably. One of these is definitely the serious lack of resources, which unfortunately characterizes Hungarian healthcare. The procurement of equipment that is significantly more important than drones often takes months, and the waiting list for some surgical procedures in hospitals is often many months long. Given these circumstances, I think I can say that the wider use of drones in healthcare is not a priority. In addition, a serious lack of human resources would cause a serious problem, since the use of these devices requires special knowledge and skills for safe operation.

4. *Closing thoughts*

The appearance of the coronavirus and the effects of the pandemic made humanity and the governments of the countries realize that more emphasis should be placed on the development of digital solutions in the field of healthcare as well. In my opinion, it can already be stated that the big winners of the

[28] See more in: B.Nemeth, M.Csanádi and Z.Kaló, *Overview on the current implementation of health technology assessment in the healthcare system in Hungary*, Cambridge University Press, 2017. Source: ww.cambridge.org/core/journals/international-journal-of-technology-assessment-in-health-care/article/abs/overview-on-the-current-implementation-of-health-technology-assessment-in-the-healthcare-system-in-hungary/03E08FF3A4C46B40CD913F0FA40A34AD#article.

[29] Source: https://www.origo.hu/techbazis/20150703-dronokkal-mentettek-eletet-tuzoltok-dron-kopter-aradas.html.

[30] Source: http://hvg.hu/tudomany/20170331_korhazi_dron_egeszsegugyi_szallitas_laborminta_gyors_szallitas_svajc_lugano.

[31] A drone has transported chilled human blood more than 250 kilometers across the hot Arizona desert – setting a record for transporting biological samples by remotely operated vehicle. The blood was still in good condition after the three-hour transport, which means that the role of drones in rural medicine can even be life-saving. Source: http://www.origo.hu/gazdasag/20170921-dronnal-szallitottak-emberi-vermintat-sikeresen.html (last viewing: 2023.03.21)

[32] Source: https://hvg.hu/itthon/20150413_Dronnal_keresnek_egy_eltunt_embert_Barany

change[33] will be, on the one hand, the technology companies implementing the developments, along with the citizens. According to my point of view, the majority of users and patients are currently showing openness and willingness to accept new digital services and devices, as they perceive their improvement in quality of life, prevention and greater security about their health. Of course, doubts can be raised regarding the protection of personal data, especially when using mobile applications, which developers and implementing governments must be able to adequately ensure. If this succeeds, the governments, including Hungary, can take new steps in the process of building a well-functioning, efficient, transparent, modern, service-providing state, which is the greatest expectation of citizens and clients.

Overall, I can say that the objectives of the developments that have taken place in my country, Hungary, are certainly worthy and correct, but I must admit that there are also visible shortcomings in the health care development system[34]. Such a large sector, which affects all citizens, requires extremely complex developments even in calm periods, let alone in an age weighed down by a pandemic. If I add to this the serious situation of the lack of funds and human resources, then it becomes clear that the current situation of the Hungarian healthcare sector, despite the introduction of digital solutions, cannot be considered completely positive. Despite all of this, I believe that with the improvement of modern devices, applications and the attitude of citizens, we can get closer to creating a better Hungarian healthcare network.

[33] See more in: P. Mihályi, *Recent changes in the hungarian healthcare system, 2010-2017*, Zdrowie Publiczne i Zarządzanie Journal, vol. 15, 2017.
[34] See more in: E. Orosz and A. Burns, *The healthcare system in Hungary*, in *OECD Economics Department Working Papers*, No. 241, https://dx.doi.org/10.1787/088362842087.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 243-248
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 19

*System of e-Health Tools. The Example of Poland**

Maciej Błażewski
(University of Wrocław)

Michał Raduła
(University of Wrocław)

ABSTRACT E-Health is the electronic transfer of information between entities of the healthcare system. The provisions of the law define the comprehensive e-Health system. This system encompasses the e-appointment, which is a remote medical consultation, and the Electronic Medical Records, which includes electronic prescriptions and electronic re-ferrals. A particular means of electronic communication is the Patient Online Ac-count, which is a module of the public ICT system used by the patient to obtain and transfer information. Technical tools, which are related to e-Health, have a positive im-pact on the situation of healthcare institutions and patients.

1. *Introduction*

E-Health is an element of technical progress. Electronic communications enable easier access to the healthcare system. This article is about medical law and the new possibilities and obligations under Polish law (as a result of digitization, e-Health in the Polish healthcare system).

New technology allows patients to obtain medical consultations remotely and to obtain a prescription or doctor's referral electronically. There was no legal basis for going to an appointment with a doctor without personal, direct contact between doctor and patient in the past. Digitization of this field makes the functioning of healthcare entities easier and increases health security for the patient (through quick consultations). Of course, digitization of the healthcare system also provides greater comfort for patients in obtaining healthcare services.

2. *E-Health*

New technology and digitization of the healthcare system are related to the functioning of healthcare entities, but the rights and obligations of the healthcare provider and the patient are also affected. Changes have been introduced into patient registration, security of medical records and the method of contact with patients and other entities within the healthcare system (hospitals etc.) and with state healthcare-system institutions (e.g. National Health Fund)[1].

E-Health is primarily about remote healthcare services[2] (e.g. medical consultations), and the ability to obtain a prescription or doctor's referral remotely. Additionally, the respective impact on the patient's actual and legal situation should be emphasized – effective access to medical assistance and remote access to medical records and test results. Technical progress in healthcare is improving the standard of medical services, and is giving patients greater access to the healthcare system while offering greater opportunities of professional training for medical staff[3].

There are currently numerous notions related to the rapid development of digitization of the healthcare system and these should be properly recognized, while some should not be interpreted as being synonymous with the concept. The notion of 'TEC' should first be presented with regard to the notion of 'E-Health'. This is an acronym of 'Technology-Enabled Care'. TEC is the broadest notion in the digitization of the healthcare system. It refers to every use of new technologies in caring for the patient. The notion of 'E-Health' is related to telemedicine

* Article submitted to double-blind peer review.

[1] National Health Fund established by the Act of 27 August 2004 on health services financed from public funds (consolidated text Journal of Laws 2021, item 1285 with amendments), hereinafter HSFPF.

[2] Serviced by health care entities – regulations based on the Act of 15 April 2011 on Medical Activity (consolidated text Journal of Laws 2022, item 2770), hereinafter AMA.

[3] M. Florczak and S. Sebastian, *Telemedycyna w polskim prawie administracyjnym,* in I. Lipowicz, G. Szpor and M. Świerczyński (eds.),*Telemedycyna i e-Zdrowie. Prawo i informatyka,* Warsaw, Wolters Wluwer, 2019.

and telehealth (which is narrower). Telehealth includes telemedicine, management procedures, monitoring procedures and the popularization of knowledge about healthcare (the meaning of telemedicine and telehealth is flexible; these terms are interconnected). The narrowest concept is telemedicine, which encompasses: 1) remote health services, 2) crossing geographical barriers – users can be in various locations during the call, 3) the use of different, new types of ICT technology (Information and Communication Technology), 4) increasing the standard of healthcare services and popularization of new treatment methods[4].

The legal basis of telemedicine in Polish law is Article 3, para. 1 of the Act on Medical Activity of 15 April 2011. Medical activity is primarily based on healthcare services. These services can be provided to the patient through ICT systems or a communication system[5]. The healthcare service is an activity for maintaining and recovering health or improving the level of health, as well as other medical activities related to medical treatment or based on other regulations[6].

It should be emphasized that the legality of telemedicine is also conditional on the regulations related to the medical professions, which are regulated, in particular, in the Act on the Medical Profession and the Act on the Profession of Nurse and Midwife. The profession of a doctor is based on the provision of healthcare services by an appropriately-qualified person (with documented qualifications). In addition to direct, personal contact, healthcare services (and other activities related to the profession of doctor, e.g. scientific research or teaching the medical profession) can be provided via ICT systems[7]. Activities related to the professions of nurse and midwife can also be performed remotely, through ICT systems[8].

E-Health, as classified in public law, is a part of the provision of public administration, which, according to the Polish doctrine of administrative law, is related to the performance by the government administration of public tasks directly and indirectly providing tangible and intangible services to the citizens[9]. Furthermore, e-Health is also a part of e-government, because of the use of electronic tools, ICT systems, for providing public services – enabling patients to effectively exercise their constitutional right to healthcare.

E-Health can be also defined as a set of ICT infrastructure and technical tools intended to provide medical care. The ICT infrastructure in Poland especially includes the Medical Information System and the Patient Online Account. This infrastructure enables patients to obtain medical information via e-consultations, as well as e-prescriptions and e-referrals.

3. *E-Appointment*

The notion of 'e-appointment' is not a normative term. It refers to the provision of medical consultations remotely, namely with the use of various types of communication tools. The legal basis of the e-appointment is Article 42, para. 1 of the Act on the Medical Profession: the doctor determines the patient's health situation after a personal examination, or after an examination through the ICT systems, as well as after analysing the patient's available medical records.

The Polish legal system has no legal definition of 'doctor's determination'. The legal doctrine refers to two senses of this notion – formal and physical. In the formal sense, it is the issuance of a certificate by a doctor, which then enables the patient to exercise some of his or her rights, based on the law (the patient's rights). In the physical sense, the doctor makes a substantive assessment, namely a statement on the patient's health and, in particular, the recommendations for further medical treatment[10].

The examination of a patient through ICT systems needs a very broad interpretation. The doctor can therefore handle the treatment remotely in any way that is effective. In particular, this can be via a phone call with the patient, consultation through an appropriate

[4] *Ibidem*.
[5] Art. 3 item 1 AMA.
[6] Art. 2 item 1 point 10 AMA.
[7] Art. 2 on the Act of 5 December 1996 on Medical Profession (consolidated text Journal of Laws 2022, item 2770).
[8] Art. 11 item 1 on the Act of 15 July 2011 on the profession of nurse and midwife (consolidated text Journal of Laws 2023, item 185).
[9] J. Jagielski, in J. Jagielski and M. Wierzebowski (eds.), *Prawo administracyjne*, Warsaw, Wolters Kluwer, 2022, 38.
[10] M. Malczewska, *Commentary on the article 42*, in *Ustawa o zawodach lekarza i lekarza dentysty*. *Komentarz*. Wydanie III, E. Zielińska (ed.), Warsaw, Wolters Kluwer, 2022.

application enabling video and audio contact, or also obtaining information (automatically created medical results) from a device that is analysing the patient's health (e.g. patient's ECG – electrocardiogram)[11]. The e-appointment also includes issuing an electronic prescription or an electronic referral[12].

In connection with the notion of 'e-appointment', it is worth clarifying a term coined by the Polish legal system during the period of the Covid-19 epidemic, namely 'teleadvice' [Polish: *teleporada*]. In order to combat the epidemic, the Polish legislator decided to enable doctors to provide healthcare services in connection with the battle against the Covid-19 epidemic through an ICT system provided by an entity subordinated to the Minister of Health responsible for healthcare information systems. This legal regulation expired because it was only established for a definite term (365 days)[13]. Teleadvice was therefore a type of e-appointment through which the healthcare service was only provided in order to battle against Covid-19. The epidemic is a dynamic threat – it resulted in some patient rights, as well as regulations on medical records not being applicable or being applicable to a narrower extent, according to the standard of the remote healthcare service.

The Polish legislator established two types of technical conditions for ICT systems used to holding e-appointments. This division is based on the status of the ICT system. The public IST system, which is only used for e-appointments (it is only used by public entities providing healthcare services), should satisfy the minimum conditions specified by law. Polish law does not lay down any special technical conditions for a private ICT system, in the sense of infrastructure used by private entities (which provide healthcare services). Therefore, if the healthcare service is being provided by an entity which does not perform public tasks, the doctor, dentist, nurse or midwife can practice their professions by providing healthcare services, including healthcare services with the use of any ICT systems, provided that they comply with the fundamental rules on this (confidentiality and safety of the information sent).

4. *The national healthcare information system.*

The National Healthcare Information System is used to process data, which are necessary, among other things, to provide health services[14]. The National Healthcare Information System is a collection of databases operating within the Medical Information System[15]. The health service provider enters electronic prescriptions and electronic referrals, as well as data from the electronic medical record, into the National Healthcare Information System[16]. The provider is also required to enter data on medical events into the Medical Information System[17]. The Medical Information System is operated by the Electronic Platform for Gathering, Analysing and Distributing Digital Resources on Medical Events, which is the public ICT (Information and Communication Technology) system[18]. This platform enables providers to access data on health services that have been provided and planned[19], as well as to exchange electronic medical records with other providers[20].

5. *The patient online account*

The Patient Online Account is a means of electronic communication used by the patient to obtain and provide information. This account is a module of the public ICT system – the Electronic Platform for Gathering, Analysing and Distributing Digital Resources on Medical Events[21]. The patient has online access to this account directly or through a

[11] *Ibidem.*
[12] Art. 95b on the Act of 6 September 2001 on Pharmaceutical law (consolidated text Journal of Laws 2022, item 2301), hereinafter PL; Art. 59aa HSFPF.
[13] Amended art. 7 item 4 on the Act of 2 March 2020 "Anti-COVID19" (consolidated text Journal of Laws 2023, item 412).
[14] Art. 1 item 1 the Act of 28 April 2011 on the National Healthcare Information System (consolidated text Journal of Laws 2022, item 1555 with amendments), hereinafter NHIS. K. Świtała emphasizes that the Medical Information System is one of the types of basic state infrastructure. K. Świtała, *System informacji w ochronie zdrowia a problematyka planowania i ewaluacji polityk zdrowotnych w Polsce*, in *Roczniki Kolegium Analiz Ekonomicznych*, Vol 52, 2018, 105.
[15] Art. 5 item 1 point 2 NHIS.
[16] Art. 11 item 5 point 1-2 NHIS.
[17] Art. 56 item 2a NHIS.
[18] Art. 5 item 2 point 2 in connection with art. 7 item 1 point 1 NHIS.
[19] Art. 7 item 1 point 1 NHIS.
[20] Art. 7 item 1 point 3 NHIS. B. Michalak, *Dokumentacja medyczna 3D*, in *Studia Ekonomiczne Uniwersytetu Ekonomicznego w Katowicach*, Vol 199, 2014, 192.
[21] Art. 2 point 19 in connection with art. 7 item 1 NHIS.

public mobile application[22].

The Patient Online Account offers two types of functions: 1. access to general information[23] or information about the legal situation of the patient (the recipient of the health service)[24]; 2. the ability to submit applications[25] and declarations[26].

Patients or statutory representatives of minor patients have access to this online account[27].

The Patient Online Account has basic standards for authorized access. These standards apply to technical and organizational requirements.

The technical standard of access to the Patient Online Account applies to the authentication of the patient or other authorized person. Two types of authentication are admissible, depending on the type of access to the account. The first, which is used for direct access to this account, is the use of electronic identification related to the National Electronic Identification Node[28]. The second is the use of a public mobile application. This type of authentication involves the use of an electronic certificate[29].

The organizational standard of access to the Patient Online Account includes blocking access for the statutory representative of the health service recipient (the patient) if his authorization for access expires[30].

6. *Electronic Health Records*

Electronic Medical Records also constitute an element of e-Health. These records are generated in connection with the provision of health services[31]. The electronic medical records include electronic prescriptions and electronic referrals.

These records are available free of charge in the public ICT system, and comply with the technical standard for ensuring data integrity and the authorization of the entity that prepared these records[32].

An electronic prescription is a document issued electronically[33]. The rule is currently to issue electronic prescriptions. The provisions of the law specify exceptions under which paper prescriptions may be issued[34].

An electronic referral is also a document issued electronically[35]. An electronic referral is issued for health services, which are specified in the list of the Minister of Health[36]. The provisions of the law also lay down the exceptions, by which a referral may be issued only in paper form, in the case of health

[22] According to art. 7b item 1a NHIS, access to the Patient Online Account can be ensured over public mobile application.

[23] Access to general information refers to inter alia data on the amount of reimbursement for medicinal products (art. 7a item 1 point 8 NHIS.); data on health prevention and healthy lifestyle, which are based on individual medical data of the service recipient (art. 7a item 1 point 15 NHIS.).

[24] Access to information about legal situation of patient related to inter alia: data on the right to health services (art. 7a item 1 point 2 NHIS.); data on issued medical certificates (art. 7a item 1 point 6 NHIS.); data on the amount of health care contribution, which is paid by the service recipient (art. 7a item 1 point 7 NHIS.); data on the service provider and the health services provided by him (art. 7a item 1 point 11 NHIS.).

[25] Applications submitted over the Patient Online Account include inter alia: an application for a European Health Insurance Card (art. 7a item 1 point 12 NHIS.); an application or a complaint to the Patient's Rights Ombudsman, the Minister of Health and the National Health Fund (art. 7a item 1 point 14 NHIS.).

[26] The Patient Online Account may be also used to: authorize a third party to access medical records (art. 7a item 1 point 3 NHIS.); sending consent to provide health services (art. 7a item 1 point 5 NHIS.); sending a declaration of choosing a health service provider (art. 7a item 1 point 10 NHIS.).

[27] Art. 7b item 2-3 NHIS.

[28] Art. 7b item 1 NHIS. in connection with art. 20a item 1 point 1 Act of 17 February 2005 on the computerization of the activities of entities performing public tasks (consolidated text Journal of Laws 2023, item 57), hereinafter CAEPPT.

[29] Art. 7b item 1a NHIS. in connection with art. 19e item 1 CAEPPT.

[30] Art. 7b item 5 NHIS.

[31] Judgment of the Supreme Administrative Court of 6 October 2020, II GSK 557/18, CBOSA. According to the judgment, electronic medical records, which include a document generated in connection with the provision of health services, is subject to authorization with electronic authorization means. See also Z. Maj, *Elektroniczna dokumentacja medyczna – wybrane aspekty prawne*, w *Przegląd Prawa Medycznego*, Vol 1, 2022, 116.

[32] According to art. 2 point 6 NHIS., the Electronic Medical Records includes electronic documents issued with a qualified electronic signature, a trusted signature, a personal signature or using the means of confirming the origin and integrity of data available in the public ICT system, which is provided free of charge by the Social Insurance Institution.

[33] Art. 95b item 1 PL.

[34] Art. 95b item 2 PL.

[35] Art. 59aa item 1 the Act of 27 August 2004 on health services financed from public funds (consolidated text Journal of Laws 2021, item 1285 with amendments), hereinafter HSFPF. The provisions of law equals an electronic referral with a referral issued in paper form (art. 59aa item 1 HSFPF).

[36] Art. 59aa item 2 HSFPF in connection with the Ordinance of the Minister of Health of 15 April 2019 on referrals issued in electronic form in the Medical Information System (consolidated text Journal of Laws 2022, item 1417).

services for which, as a rule, an electronic referral is issued[37].

The provisions of the law define a uniform model for transferring information on electronic prescriptions and electronic referrals, as well as the security standards regarding these documents.

There are two levels of data transfer related to electronic medical records. These are the provision of access to electronic medical records and the distribution of information about these records.

The first level, which involves the provision of access to electronic documentation, is passive in nature. This level includes enabling authorized personnel to view these records, which are stored in a public ICT system. Electronic prescriptions and electronic referrals are simultaneously recorded in the Medical Information System[38] and are then made available through this system[39]. The objective of providing access to this documentation is to provide a technical tool to the authorized person enabling the use of this system.

The second level, which involves the provision of information on electronic medical records, is active in nature. This information is received by authorized personnel. Information related to these electronic medical records includes data which are necessary for authorizing the use of the documents. This information also includes the data of the persons issuing these documents and the data of the addressees of these documents[40]. Information on electronic prescriptions also includes data on the medication and its use[41], as well as information on whether the patient is entitled to receive the medication free of charge[42]. This information may be sent to the addressee by e-mail or by text messages, as well as in the form of a printout[43]. The provision of information on electronic medical records is a technical activity of a declaratory nature. The objective of providing information on this documentation is to transfer it to an authorized person.

The provisions of law lay down the security standards for electronic prescriptions and electronic referrals[44]. These standards apply to the authorization to issue these documents and maintain their integrity. The standard for authorizing the issuance of these documents is the requirement that they are signed with a qualified electronic signature, a trusted signature, a personal signature, or another public means of electronic authorization[45]. The standard for maintaining the integrity of electronic prescriptions and electronic referrals includes a special procedure for changing their content. An effect of this change is the cancellation of the original version of the electronic prescription or electronic referral and the issuance of a new prescription or new referral[46]. The objective of this procedure is to ensure that the doctor or other person issuing these documents has control over their content.

The provisions of the law also lay down the regulation on setting the technical requirements for Electronic Medical Records. The Minister of Health defines the formats of Electronic Medical Records[47], as well as the standards for exchanging these medical

[37] Art. 59aa item 3 HSFPF.
[38] Art. 96a item 9a PL, and art. 59aa item 5 in connection with art. 59aa item 2 HSFPF.
[39] Art. 11 item 2 NHIS. A. Klich, *Wybrane zagadnienia prawne elektronicznej dokumentacji medycznej*, w *Ekonomiczne Problemy Usług*, Vol 1, Issue 2, 2017, 355. According to art. 59b item 2b HSFPF, the Internet Patient Account ensure access to the electronic referral.
[40] Art. 96b item 1 PL and art. 59b item 1 HSFPF.
[41] Art. 96b item 1 point 10-14 PL.
[42] (art. 44a item 3 in connection with art. 44a item 1 and art. 44b item 2 in connection with art. 44b item 1 the Act of 12 May 2011 on the reimbursement of medicines, foodstuffs intended for particular nutritional uses and medical devices (consolidated text Journal of Laws 2022 item 463 with amendments).
[43] Art. 96b item 2 PL in connection with art. 7 item 1 NHIS., and art. 59b item 2 HSFPF in connection with art. 7 item 1 NHIS.
[44] A. Klich emphasizes that the Electronic Medical Record ensures greater data security compared to the documentation issued in paper form. A. Klich, *Wybrane zagadnienia prawne elektronicznej dokumentacji medycznej,* in *Ekonomiczne Problemy Usług*, Vol 1, Issue 2, 2017, 352. The similar stance was expressed by J. Pacian, A. Pacian, T. B. Kulik, A. Stefanowicz, H. Skórzyńska, D. Żołnierczuk-Kieliszek, M. Janiszewska, *Ochrona danych medycznych zawartych w dokumentacji medycznej a wykorzystanie bezpiecznego podpisu elektronicznego*, in *Zdrowie Publiczne i Zarządzanie*, Vol 10 (B), 2012, 194.
[45] Art. 96a item 1 point 3 PL and art. 2 point 6 letter c NHIS. in connection with art. 59aa item 2 HSFPF. Judgment of the Supreme Administrative Court of 6 October 2020, II GSK 557/18, CBOSA. According to this judgment, the requirement to use a means of electronic identification (electronic signature) is the result of the digitization of the Electronic Medical Records. See also E. Kawiak-Jawor, M. Kaczoruk, P. Kaczor-Szkodny and E. Dudzińska, *Bezpieczeństwo danych medycznych w kontekście wdrożenia elektronicznej dokumentacji medycznej*, in *Medyczna Wokanda,* Vol 9, 2017, 130.
[46] Art. 96a item 9b PL and 59aa item 6 HSFPF.
[47] Art. 11 item 1a NHIS.

records[48]. These requirements are published in the Public Information Bulletin[49].

7. *Conclusions*

The healthcare system in Poland has been partially digitized. Information on health services may be transferred electronically. The provisions of the law distinguish the level of interference in the manner of this communication. A significant amount of interference applies to the gathering and transfer of the Electronic Medical Records. These activities can take place through the Medical Information System. A slight amount of interference applies to the requirements for remotely providing medical consultations. The entities providing healthcare services can freely choose the ICT system or communication system over which these services are provided. However, an e-appointment will not replace comprehensive medical assistance provided after a personal examination of the patient. Therefore, the scope of health services provided remotely should be limited proportionally to the patient's needs. The digitization of the healthcare system is an important value for society. Nevertheless, the priority should be safety of life and health in connection with the provision of the health service.

[48] Art. 11 item 1b NHIS.
[49] Art. 11 item 1a-1b NHIS.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 249-266
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 20

*Health and Disablement Among Social Security Recipients in the UK: The Role of Digital Communication and Capacity in Assessments and Entitlements**

Neville Harris
(Emeritus Professor of Law at University of Manchester, UK)

ABSTRACT Large numbers of UK citizens whit health issues or disabilities currently receive financial support from the social security system by reason of having either a limited capability for work due to a physical or mental problem or a disability that significantly limits their mobility or capacity for self-care. In the UK, where a transformation to 'digital by default' has been a core services policy over the past decade, digital technology plays a hugely important role in the delivery of these and other social security benefits. It features prominently in the ways in which benefit claimants are expected to inter-act with the administrative authorities, including when they need to notify the authorities of any change in their condition which could be material to their benefit award. Covering both legal and administrative dimensions, this article critically analyses the role and impact of digital technology and digital capacity in the processes for claiming the health-related and disability-related social security benefits, in the assessments of entitlement, and in the notification of changes in circumstances relevant to entitlement.

1. *Introduction*

The UK has a wide range of social security benefits which aim to provide financial assistance for people with long-term health problems or disabilities. Some of these benefits deliver an enhanced form of out-of-work support while others are intended to help with the additional costs faced by those with care needs or mobility problems arising from physical and/or mental disability, regardless of their employment status. There is also social security support for a family member who provides day-to-day care for a severely disabled person. The relevant benefits are administered by the Department for Work and Pensions (DWP), on behalf of the Secretary of State for Work and Pensions. In the administration of what continues to be a complex benefits framework, with over 10 million health-related or disability-related benefit awards currently in payment (some people being in receipt of more than one benefit),[1] the UK Government has made

* Article submitted to double-blind peer review.

[1] The relevant benefits are described below. In Great Britain (therefore excluding Northern Ireland) these are the individual benefit totals (in millions): Personal Independence Payment 3.3m, Employment and Support Allowance 1.6m, Disability Living Allowance 1.3m, Carer's Allowance 1.4m, Attendance Allowance 1.6m and Universal Credit (UC) 6.2m (of which 27% (approx. 1.7m) were claimants with a health or disability-related entitlement): DWP, DWP Benefit Statistics August 2023 (at www.gov.uk/government/statistics/dwp-benefits-statistics-august-2023/dwp-benefits-statistics-august-2023); Universal Credit statistics, 29 April 2013 to 12 October 2023 (at www.gov.uk/government/statistics/universal-credit-statistics-29-april-2013-to-12-october-2023/universal-credit-statistics-29-april-2013-to-12-october-2023); DWP, UC Health Caseload (December 2023) (https://stat-xplore.dwp.gov.uk/webapi/jsf/tableView/tableView.xhtml); and DWP, Official Statistics: Personal Independence Payment: Official Statistics to October 2023 (DWP, 2023), at www.gov.uk/government/statistics/personal-independence-payment-statistics-to-october-2023/personal-independence-payment-official-statistics-to-october-2023#:~:text=Latest%20figures%20for%20normal%20rules,were%20assessed%20received%20an%20award(all sites accessed 16 March 2024). These figures exclude the new disability payments being phased in in Scotland (see below), where the new Child Disability Payment was being received by an estimated 13,200 children as at 30 June 2022 and the Adult Disability Payment was being received by 55,535 people at the end of April 2023: Social Security Scotland, Child Disability Payment: high level statistics to 30 June 2022, at www.gov.scot/binaries/content/documents/govscot/publications/statistics/2022/08/child-disability-payment-high-level-statistics-to-30-june-2022/documents/child-disability-payment-high-level-statistics-to-30-june-2022/child-disability-payment-high-level-statistics-to-30-june-2022/govscot%3Adocument/Child%2BDisability%2BPayment%2B-%2BPublication%2B-%2BAugust%2B2022.pdf and Adult Disability Payment high level statistics to 30 April 2023, at www.gov.scot/binaries/content/documents/govscot/publications/statistics/2023/06/adult-disability-payment-high-level-statistics-to-30-april-2023/documents/adult-disability-payment-high-level-statistics-to-30-april-2023/adult-disability-payment-high-level-statistics-to-30-april-2023/govscot%3Adocument/Adult%2BDisability%2BPayment%2B-%2BPublication%2B-%2BJune%2B2023.pdf.

uneven progress over the past two decades towards a system that is 'digital by default' in terms of its internal operation and claimant and administration interactions.

Digitalisation has, among other things, presented an opportunity for greater administrative efficiency but also, from the claimant's perspective, for easing the process of claiming benefits and providing a more effective channel through which to report relevant changes in circumstances, such as a marked improvement or decline in health. There is an onus on the claimant to report such changes in order to ensure that an ongoing benefit award continues to be commensurate with their level of need. Unless the DWP is made aware of relevant changes there is a risk that the level of award could be incorrect. If it exceeds the correct entitlement based on the individual circumstances – and particularly if there is an extended period of time before the DWP is made aware of the change – the claimant may accumulate a significant amount of overpayment, which could be subjected to recovery by the Secretary of State.[2] As discussed below, many thousands of notifications of changes in circumstances, including changes in health or disability, are made to the DWP each year. Dealing with them, which may involve making a new decision on a claim, is a very important aspect of benefit administration.

Before examining this issue as it relates to changes in health or disability and the role of digital processes in this context, it is necessary to outline the relevant and health-related and disability-related social security benefits in the UK.

2. *Entitlement to Social Security Benefits Related to Health or Disability*

Within the UK social security system a distinction may be drawn between benefits to support people who have a limited capability for work due to their physical or mental condition, and benefits for people with a disabling condition which gives rise to additional needs by limiting their mobility or the capacity to undertake aspects of daily living without support and care from another person. (But it should be noted that a majority of people receiving a limited capability for work benefit *also* receive a disability benefit.[3]) There is also a separate allowance paid to carers of severely disabled people. The outline below explains the relevance and methodology of current health and disability assessments and how digital capability in health/disability is reflected in some of the prescribed assessment criteria.

2.1 *Limited capability for work due to a physical and/or mental condition*

What began as an insurance-based sickness benefit under the Beveridge reforms of the late 1940s[4] is now a partly insurance-based (contributory) and partly assistance-based (means-tested) scheme of social security for people whose ability to work is compromised by physical and/or mental ill-health. The main benefit in this field has been Employment and Support Allowance (ESA). When first introduced (in 2008) this benefit was available in two forms: (i) as an insurance benefit (*contributory ESA*), with entitlement not based on a means test but primarily dependent on a record of National Insurance contributions, giving entitlement normally for only the first 365 days of a period of limited capability for work; and (ii) as a means-tested (income related) benefit (*income-related ESA*) for persons with a limited capability for work who had exhausted their entitlement to contributory ESA or who did not have a sufficient contributions record.[5] After further reforms in 2012 and 2013,[6] while contributory ESA remained in place (although is now referred to by the DWP in some contexts as "'new-style' ESA"), income-related ESA has been replaced for new claims by Universal

[2] This will be done under the framework of rules set out in the Social Security (Payments on account, Overpayments and Recovery) Regulations 1988 (SI 1988/664) (as amended).

[3] DWP, Health and Disability benefits based on data from 2019 to 2022 (DWP, 2023) at www.gov.uk/government/statistics/health-and-disability-benefits-based-on-data-from-2019-to-2022/health-and-disability-benefits-based-on-data-from-2019-to-2022.

[4] See N. Harris, *Beveridge and Beyond: the Shift from Insurance to Means-testing*, in N. Harris *et al., Social Security Law in Context*, Oxford, Oxford University Press, 2000, 87-117.

[5] See N. Harris and S. Rahilly, *Extra Capacity in the Labour Market?: ESA and the Activation of the Sick and Disabled in the UK*, in S. Devetzi and S. Stendahl (eds.), *Too Sick to Work? Social Security Reforms in Europe for Persons with Reduced Earnings Capacity*, Alphen aan den Rijn, Wolters Kluwer, 2011, 43-75.

[6] Principally, the Welfare Reform Act 2012; the Universal Credit Regulations 2013 (SI 2013/376); and the Employment and Support Allowance Regulations 2013 (SI 2013/379).

Credit (UC)[7] for those with a limited capability for work (*limited capability UC*).[8]

2.1.1. *Assessment of limited capability for work*

For both ESA and limited capability UC, entitlement is normally determined (after an initial period) on the basis of an assessment – a Work Capability Assessment (WCA) – carried out by a healthcare professional. Exceptionally, the DWP may decide a claim simply on the basis of information submitted by the claimant, in particular via the questionnaire form provided by the DWP. This form is available online but has to be signed and sent by ordinary mail to the Department.[9]

Claimants found to have a limited capability for work due to their mental and/or physical problem(s) will be allocated to one of two groups. The first comprises those who also have a limited capability to undertake a 'work-related activity' (see below), and thus a more severe degree of incapacity for work. Persons in this category are placed in the ESA 'support group' (or the equivalent under limited capability UC), which means they will not have to undertake work-related activities such as attending meetings at a jobcentre or possibly attending training on such matters as basic mathematics as a condition of receiving the benefit. The others will be allocated to the ESA 'work related activity group', receiving a lower rate of benefit, and will be expected to undertake some work preparation activities and attend interviews. Currently just over 60 per cent of new ESA claimants are placed in the support group following their initial WCA.[10]

During 2020 and 2021, due to the Covid-19 pandemic, face-to-face WCAs did not take place. Although some have since resumed, the assessment agencies[11] have been operating "a predominantly virtual assessment channel", with mostly telephone-based interviewing.[12] For example, in the year to March 2023, 66 per cent of WCAs were by telephone, 7 per cent via video, 13 per cent were paper-based and 14 per cent were face to face, repeating a pattern seen over most of the preceding twelve months apart from January 2022, when a Covid-19 wave led to 80 per cent of assessments being via telephone and there were no face to face assessments.[13]

The WCA is not without controversy. In particular, there is concern about the accuracy of the assessments and the mental strain the process causes claimants in general, in both waiting for and then undergoing the health assessment.[14] Evidence suggests that telephone or video health or disability assessment processes are more, rather than less, stressful for some claimants than face-to-face in-person assessment; and there is also a risk that communication barriers can affect the claimant's direct participation.[15] Consequently, the Work and Pensions Committee of the House of Commons has recommended that claimants be given a choice of mode for the assessment.[16]

The WCA focuses on a range of individual activities, prescribed in regulations,[17]

[7] UC not only replaced Income-related ESA but also Income-based Jobseeker's Allowance and Working Tax Credit. Indeed, UC is now the principal means-tested benefit in the UK for the out-of-work or workers with a low income: see P. Larkin, *Universal Credit, "Positive Citizenship", and the Working Poor: Squaring the Eternal Circle?*, in *Modern Law Review,* vol. 81, no. 1, 2018, 114-131.

[8] Claimants of contributory ESA who are in the 'support group' (see below) can continue to receive the benefit for longer than 365 days, however: Welfare Reform Act 2007, ss 1A and 1B.

[9] The UC form (form UC50) is available at www.gov.uk/government/publications/uc50-form-universal-credit-capability-for-work-questionnaire. For the ESA version (ESA50), see www.gov.uk/government/publications/capability-for-work-questionnaire

[10] DWP, ESA: outcomes of Work Capability Assessments including Mandatory Reconsiderations and Appeals: March 2024, at www.gov.uk/government/statistics/esa-outcomes-of-work-capability-assessments-including-mandatory-reconsiderations-and-appeals-march-2024/esa-work-capability-assessments-mandatory-reconsiderations-and-appeals-march-2024.

[11] WCAs are currently carried out under contract to the DWP by Maximus.

[12] Stuart Paterson, Client Executive Partner, Independent Assessment Services (Atos), Oral Evidence to Work and Pensions Committee, 25 May 2022, Q277 and Antony King, Managing Director and Client Partner of Capita Health & Welfare, Capita, Q 285.

[13] Written Answer, House of Commons, 9 March 2023, at https://questions-statements.parliament.uk/written-questions/detail/2023-03-09/162178.

[14] See for example, Work and Pensions Committee, *PIP and ESA assessments*, 7th Report of Session 2017–2019 (HC 829), London, House of Commons, 2018; and Work and Pensions Committee, *Health assessments for benefits*, Fifth Report of Session 2022–23 (HC 128), London, House of Commons, 2023.

[15] *Ibid.* (2023), par. 41-42.

[16] *Ibid.*

[17] Employment and Support Allowance Regulations 2013 (SI 2013/379) Schedules 2 and 3; Universal Credit Regulations 2013 (SI 2013/376) Schedules 6 and 7; and see also the ESA Regulations 2008 (SI 2008/794) Schedules 2 and 3 for claimants still in receipt of Income-related ESA under transitional arrangements.

spanning 17 functional areas. Examples include "mobilising", "standing and sitting", "reaching" and "coping with change". An inability in relation to any of them must stem from "a specific bodily disease or disablement" or, in the case of mental disability, from a "specific mental illness or disablement".[18] Each activity is broken down into specific abilities, identified by individual descriptors to which specific numbers of points (either 0, 6, 9 or 15) are attached. A claimant scoring a total of 15 points or more from one or more of the different descriptors is classed as having a limited capability for work (although in exceptional cases someone with less than 15 points can be treated as meeting the requirement, such where facing a substantial health risk if classed as not having a limited capability for work).

In the light of this paper's focus, it is significant that some of the WCA descriptors relate, or can be related, to digital or information technology (IT) functions. For example, for "standing and sitting", nine points would be scored for an inability to remain at a work-station (whether standing and/or sitting) for more than 30 minutes before needing to "move away in order to avoid significant discomfort or exhaustion". Nine points would also be scored, in relation to "manual dexterity", where the claimant "cannot single-handedly use a suitable keyboard or mouse", while an inability to press a button (such as on a telephone) with either hand would score 15 points.[19] Some of the descriptors that have a more general application, particularly those related to mental factors such as cognitive capacity (for example, the mental ability to learn how to use a device),[20] may also be relevant to a person's digital capabilities.

The reference to a *single-handed* use of a keyboard or mouse was inserted into the regulations in 2012 in order to reflect an intention that the assessment of manual dexterity should focus on simple hand and wrist function. Appeal tribunals had previously been awarding points to claimants on the basis of the standard use of a keyboard requiring two hands.[21] In *DW v Secretary of State for Work and Pensions*, for example, the appellant could not use the shift function on the keyboard while, for example, typing '@' with the other hand. Upper Tribunal Judge May held that it was necessary to take a broad approach rather than merely relying on the fact that the appellant could physically press a keyboard key.[22] Subsequently, in *CL v Secretary of State for Work and Pensions*, Upper Tribunal Judge Mark followed a similar line, noting that "it would plainly be much harder to operate a keyboard with only one hand rather than with two" and that "combinations of three keys, such as control, alt and delete, would seem to be excluded at least on a conventional keyboard"; he said it might be reasonable to conclude that "the claimant could not properly be described as able to use a suitable keyboard using only one hand which would also need to operate the mouse". [23] However, in *KH v Secretary of State for Work and Pensions*, Judge Mark took a slightly different approach. A claimant with the use of only one hand had been considered able to operate a keyboard with it using standard facilities such as 'StickyKeys'. While such facilities would not help in situations where it was necessary to use the mouse and a keyboard concurrently, "the fact that some uses were beyond her physical abilities would not mean that she could not use the keyboard or mouse".[24]

The question of whether the reference to an inability to use a "keyboard or mouse" meant that an ability to use one but not the other would prevent the descriptor from being met was answered in the affirmative in *DG v*

There has recently been a consultation over proposed changes to some of the activity descriptors: see DWP, *Work Capability Assessment: activities and descriptors* (CP 930), London, DWP, 2023, at www.gov.uk/government/consultations/work-capability-assessment-activities-and-descriptors/work-capability-assessment-activities-and-descriptors. Some changes are planned as a result: DWP, *Government Response to the Work Capability Assessment: Activities and Descriptors Consultation* (CP 973), London, DWP, 2023.

[18] ESA Regs 2013, reg. 15(5); UC Regs 2013, reg. 39(4); UC Regs 2008, reg. 19(5).

[19] ESA Regs 2008, Sch 2 par. 5(a) and (d); ESA Regs 2013, Sch 2 par. 5(a) and (d); UC Regs 2013, Sch 6 par. 5(a) and (d).

[20] *Ibid*. (all), par. 11 of each of the Schedules, which refers to the activity of 'learning tasks'.

[21] See DWP, *Explanatory Memorandum to the Employment and Support Allowance (Amendment) Regulations 2012 2012 No. 3096* (2012) at www.legislation.gov.uk/uksi/2012/3096/pdfs/uksiem_20123096_en.pdf.

[22] *DW v Secretary of State for Work and Pensions (ESA)* [2010] UKUT 245 (AAC).

[23] *CL v Secretary of State (ESA)* [2013] UKUT 0434 (AAC), par. [7] and [8].

[24] *KH v Secretary of State (ESA)* [2014] UKUT 0455 (AAC), par. [14].

Secretary of State for Work and Pensions.[25] The appellant had broken his left hand, damaging the nerve endings, and had had a pin inserted, leaving the hand weak and without a grip. He could therefore only use one hand. Judge Wright said that the claimant's ability to use a mouse was sufficient to deny him the nine points he had sought. He also concluded that an ability to use a keyboard meant having a simple ability to type out letters, numbers and symbols rather than an ability use it fully, for example typing sentences beginning with a capital letter.[26]

The overall effect of the case law and regulatory amendments is therefore that while inability to use a keyboard or mouse can go a substantial way towards securing entitlement to ESA or limited capability UC, the threshold for such inability has been set at quite a high level and will not be reached if there is a simple, even if limited, functional ability.

2.1.2. *Assessment of limited capability for work-related activity*

A separate set of activities is prescribed for the assessment of a limited capability for work-related activity. Here the assessment is not points-based. To qualify as having this limitation the claimant merely has to satisfy any *one* of the set descriptors (or will qualify if there is a substantial risk to physical or mental health if they were classed as not having this limited capability). One descriptor, for example, refers to an inability to press a button using either hand.[27] Someone with this limitation would satisfy the tests for both limited capability for work (as this inability scores 15 points) and limited capability for work-related activity. They would therefore be placed in the 'support group' category of entitlement.

2.2. *Due to physical or mental disability, a need for assistance with daily living activities or mobility*

The UK has been described as "somewhat unusual in its provision for disabled people and the people who care for them compared with other countries", by reason of its provision of entitlement to specific universal non-contributory cash benefits providing assistance towards the additional economic costs arising from disability and long term health problems, particularly in relation to mobility or personal care for daily living.[28] Despite several key reforms over the past three decades the essential aims and structures of this area of support within the social security system have continued.[29]

2.2.1. *The main disability benefits*

Currently over six million awards of the main disability benefits are in payment to people in Great Britain.[30] The benefits, none of which is a means-tested benefit or contributory benefit, comprise:

(1) Personal Independence Payment (PIP) − the principal disability benefit for claimants aged 16 or over and under retirement pension age;

(2) Disability Living Allowance (DLA) − now available only for under-16 year olds (but some older people continue to receive it under pre-existing awards although will eventually be moved onto PIP); and

(3) Attendance Allowance (AA) – which is confined to people of retirement age.

Entitlement to AA is based on having a need for "attention" − personal assistance, which can be mental or physical − from another person frequently during the day, or repeatedly at night, in connection with bodily functions. Alternatively, the claimant may need a substantial level of supervision during the day or night from another person in order to avoid being in or causing substantial danger. AA claimants who need any such degree of support by both day *and* night receive the higher of two rates of the allowance; those who need the support only by day *or* at night qualify for a lower rate.[31]

While AA basically only covers care needs, DLA has two separate components, one in respect of care and the other covering mobility. Claimants can qualify for either or both of these components.[32] There are three levels of the care component. The top two are

[25] *DG v Secretary of State for Work and Pensions* (ESA) [2014] UKUT 0100 (AAC).
[26] *Ibid.*, par. [48] and [52]-[54].
[27] See for example ESA Regs 2013, Sch 3 par. 5.
[28] R. Sainsbury, *Disabled people and carers*, in J. Millar and R. Sainsbury (eds.), *Understanding Social Security*, 3rd ed., Bristol, Policy Press, 2018, 59-77, 59.
[29] See N. Harris, *Welfare Reform and the Shifting Threshold of Support for Disabled People,* in *Modern Law Review,* vol. 77, no. 6, 2014, 888-927.
[30] See n. 1 above.
[31] Social Security Contributions and Benefits Act 1992, ss 64 and 65.
[32] *Ibid.*, ss 71-73.

equivalent to the AA care levels, but the third is a lower level award for people needing help for a "significant portion of the day" or whose disabilities would prevent them from being able to cook a main meal for one. The mobility component is at two levels: a higher rate for those who are unable or "virtually unable" to walk or who have a prescribed condition (for example, being blind), and a lower rate for people needing guidance and supervision from another person, most of the time, when mobilising outdoors.[33]

PIP similarly has mobility and care ("Daily Living") components. The Daily Living component has only two rates – a "standard" rate and an "enhanced" rate. Like DLA, PIP has a required period condition: the claimant must, in effect, have had their disability-related limitation for the three months preceding the date of the award and be expected to continue to have it for the next nine months.[34]

Over the past few years there has been a surge in new claims for PIP. They doubled between July 2021 and July 2022, for example, increasing across all age groups and medical conditions.[35] One third of PIP claims relate to a mental health condition.[36] The three most common conditions affecting PIP claimants are currently: psychiatric disorder (38% of claims); musculoskeletal disease (general or regional) (32%); and neurological disease (12%).[37] Reporting the upward trend in claims, Joyce et al speculate that it is likely to be a reflection of worsening health rates, particularly as this growth in claims has coincided with a significant increase in the number of people with health conditions affecting their normal day-to-day activities.[38] However, the current cost of living crisis could well be another factor, driving people to look for additional sources of income. Furthermore, in the case of mental disability, the reduced stigma and increased openness about mental illness may have made people less reluctant to seek benefit on the basis of mental disablement.

In Scotland, while control of some areas of social security (including ESA and UC (above)) has been reserved to the UK Parliament under a devolution settlement, some social security law making powers have been extended to the Scottish Parliament, most notably in relation to disability benefits.[39] Scotland is using its power to begin replacing DLA (for children), PIP and AA with, respectively, Child Disability Payment (launched in November 2021), Adult Disability Payment (launched in August 2022) and Pension Age Disability Payment (due to launch in 2024),[40] although the aims and basic scope of the existing benefits will, initially at least, be preserved in their replacements.

2.2.2. *Disability assessments*

A feature of PIP that distinguishes it most from AA and DLA is that the assessment of disability-related need is based on a much more detailed set of prescribed criteria or descriptors. The assessment involves the use of a points scoring system – a similar model of assessment to that used for the WCA (above).[41] Also in common with the WCA, the assessments are mostly conducted remotely by telephone or video.[42] In 2022, 75 per cent of PIP assessments were carried out this way.[43]

[33] *Ibid.*, s. 73. In the case of a child, the child must need substantially more such guidance or supervision than children of his or her age who do not have the disability, or children without the disability would not need this guidance or supervision.

[34] Social Security (Personal Independence Regulations 2013 (SI 2013/377), regs 12-15. In the case of DLA, the prescribed periods are three and six months respectively: Social Security Contributions and Benefits Act 1992, s2 72 and 73.

[35] R. Joyce, S.R. Chaudhuri and T. Waters, *The number of new disability benefit claimants has doubled in a year*, London, IFS, 2022.

[36] *Ibid*.

[37] PIP statistics, n. 1. above.

[38] Joyce *et al.* n. 35 above, 9-12.

[39] See M. Simpson, *Social Citizenship in an Age of Welfare Regionalism: The State of the Social Union*, Oxford, Hart, 2022, 80-81.

[40] See the Social Security (Scotland) Act 2018 and the Disability Assistance for Children and Young People (Scotland) Regulations 2021 (SSI 2021/174); Disability Assistance for Working Age People (Scotland) Regulations (SSI 2022/54). See also Disability and Carer Benefits Expert Advisory Group, *Beyond a safe and secure transfer*, Edinburgh, Scottish Government, 2022, at www.gov.scot/binaries/content/documents/govscot/publications/independent-report/2023/03/disability-carer-benefits-expert-advisory-group-beyond-safe-secure-transfer/documents/disability-carer-benefits-expert-advisory-group-beyond-safe-secure-transfer/disability-carer-benefits-expert-advisory-group-beyond-safe-secure-transfer/govscot%3Adocument/disability-carer-benefits-expert-advisory-group-beyond-safe-secure-transfer.pdf.

[41] Welfare Reform Act 2012, Part 4 and the Social Security (Personal Independence Regulations 2013 (SI 2013/377).

[42] PIP assessments are organised regionally and are carried out under contract by Capita and Atos Independent Assessment Services.

[43] https://questions-statements.parliament.uk/written-questions/detail/2022-11-02/77643.

Issues arising from remote health and disability assessments were discussed earlier.

Assessments concerning the Daily Living component of PIP are focussed on ordinary personal actions such as taking nutrition, getting dressed/undressed and bathing and are not easily relatable to use of a computer or other digital device. However, a need for assistance via an aid or appliance (beyond glasses or contact lenses) or prompting, in order to read or understand basic or complex information, will score points under the criteria; and an inability to "read or understand signs, symbols or words at all" would, in itself, be sufficient to qualify the claimant for the standard rate of the component.[44] It would not matter if, for example, a PIP claimant with sight or mental processing problems could rely on *verbal* transmission of written text (that is, speaking mode) on a digital device if one of the assessment criteria that are related to "Reading and understanding signs, symbols and words" is satisfied.

At the same time, a claimant with mental health difficulties which include severe social anxiety but who is able to communicate with another person using a digital device could still score points under the assessment, for difficulties with "engaging with other people face to face",[45] since it is accepted that this refers to being able to "engage socially".[46] In a case before the Upper Tribunal where this issue arose, Judge Rowley said:

"I am quite unable to see how a claimant's ability to use a phone to send texts could possibly demonstrate an ability to engage with other people 'face to face', not least because one of the requisite criteria of an ability to 'engage socially' is an ability to understand body language".[47]

Similarly, a person who has problems with speech or hearing could qualify for points for inabilities in "communicating verbally" even if they can communicate by digital device.[48] As Judge Gray held in one case where a claimant with such difficulties could communicate using WhatsApp and texting and could use the internet, "the ability to read and write play no part in an assessment of communicating verbally under [this] activity… Accordingly an ability to use the telephone for text functions is irrelevant, albeit that in practice it may enable effective communication".[49]

2.3. *Caring for a severely disabled person*

Another important UK-wide disability-related benefit is Carer's Allowance, currently being paid to 1.4m people.50 It is intended to assist people aged 16 or over who provide a substantial amount of care for a very disabled person. The carer's caring responsibilities will limit their earning potential, but it is not clear whether the allowance is aiming to be an earnings replacement benefit per se or compensation for the extra cost of caring for a person with disabilities.[51] Entitlement[52] is conditional on being "regularly and substantially" engaged in caring for a "severely disabled person", meaning the provision of not less than 35 hours of care for that person per week.[53] The carer must be neither in full-time education nor gainfully employed (that is, in work paying more than £139 per week[54]). People resident in Scotland who receive the Carer's Allowance are also entitled to a supplement pending the introduction of a new "Carer's Assistance" benefit in that jurisdiction.[55]

3. *Digital Transformation: Social Security in the UK*

3.1. *A. Digital welfare state*

Turning now to the wider context of welfare state provision in the UK, the use of IT is of course fundamental to the management and delivery of administratively complex service systems such as the social security system. The 'machine bureaucracies' that administer social security benefits and

[44] Social Security (Personal Independence Regulations 2013 (SI 2013/377), Schedule 1 par. 8(c).
[45] *Ibid.* par. 9.
[46] See *HA v SSWP (PIP)* [2018] UKUT 56 (AAC), par. [13].
[47] *Ibid.*, at [19].
[48] Social Security (Personal Independence Payment) Regulations 2013 (SI 2013/377), Schedule 1 par. 7.
[49] *EG v Secretary of State for Work and Pensions (PIP)* [2017] UKUT 101 (AAC), [65].
[50] See note 1 above.
[51] See Sainsbury n. 28 above, 73-74.
[52] Social Security Contributions and Benefits Act 1992, s.70. A severely disabled person for this purpose is someone for whom AA, middle or higher care DLA care component or standard or enhanced rate PIP Daily Living component is payable: *ibid.* s.70(2).
[53] Social Security (Invalid Care Allowance) Regulations 1976 (SI 1976/409), reg. 4.
[54] *Ibid.*, reg 8. This limit is periodically adjusted.
[55] See the Social Security (Scotland) Act 2018, s. 81.

reach vast numbers of entitlement decisions on claims each year have long favoured the kind of standardised and automated processes for which IT systems are particularly well suited. Increasingly, this role of IT has been integral to the design not only of the processes for administration and data storage but also of the benefits themselves. The majority of areas of social security in the UK are rule-based, with legal rules setting out fairly precise criteria to be employed in determining entitlement in individual cases. IT systems are expected to enable rule-based decisions to be made in a consistent and efficient manner. In the context of social security administration, the efficiency of IT systems has, however, been significantly sub-optimal,[56] at times insufficiently cutting-edge to cope with benefit reforms and the need for a proper linking up of different parts of the very complex social security and welfare machinery. Moreover, automated and algorithmic processes for determining benefit entitlement can lead to unjust outcomes in individual cases,[57] with the risk of a repeated effect on a potential multiplicity of like cases,[58] making them susceptible in either case to irrationality-based public law challenges.[59]

The digital welfare state is, nonetheless, firmly established. Its entrenchment spans the administration of benefits – not least with the ongoing development of automated and algorithmic decision-making – but perhaps especially with the outward-facing role of IT in managing communication flow between claimants and the administration[60] and, via inter-active platforms, facilitating public information and guidance.[61] For example, in relation to the State Pension (currently paid from the age of 66, rising to 67 by 2028), the DWP plans that customer interaction should "continue to be shifted to the online channel, reducing workloads for agents by automating processes and enabling citizen straight through processing (no agent intervention) for reporting online change of circumstances", giving rise to "process efficiencies".[62] The point about the reporting of any change of circumstances is important and will be returned to later.

Against a government services policy background of "digital by default",[63] the introduction of Universal Credit as the principal and overarching income maintenance benefit in the UK for both the out-of-work – including those with a long-term incapacity for work due to ill health (as

[56] For criticism, see for example, House of Commons Public Accounts Committee, *Underpayments of the State Pension* (HC 654), London, House of Commons, 2022, par. 6-8.

[57] As Hansen et al have found in the context of the Norwegian benefits system, algorithms used in administration of social security may not always fit everyone's situation: H-T. Hansen, K. Lundberg, and L.J. Syltevik, *Digitalization, Street-Level Bureaucracy and Welfare Users' Experience,* in *Social Policy & Administration*, vol. 52, no. 1, 2018, 67-90. Such algorithms can also perpetuate inbuilt social biases and prejudices: see S.M. Appel and C. Coglianese, *Algorithmic Administrative Justice*, in M. Hertogh, R. Kirkham, R. Thomas and J. Tomlinson (eds), *The Oxford Handbook of Administrative Justice*, Oxford, Oxford University Press, 2021, 481, 496.

[58] As Fay Henman says, if algorithms are erroneous, they will be "consistently erroneous" affecting multiple cases: P.W. Fay Henman, *Administrative Justice in a Digital World: Challenges and Solutions*, in M. Hertogh, R. Kirkham, R. Thomas and J. Tomlinson (eds), *The Oxford Handbook of Administrative Justice*, Oxford, Oxford University Press, 2021, 459, 467. See also P. Henman, *Digital technologies and artificial intelligence: A computer science perspective*, in M. Adler (ed.), *A Research Agenda for Social Welfare Law, Policy and Practice,* Edward Elgar, 2022, 265, 269.

[59] J Maxwell, *Judicial Review and the Digital Welfare State in the UK and Australia*, in *Journal of Social Security Law*, vol. 28, no. 2, 2021, 94-109. For legal challenges in the UK, see *Secretary of State for Work and Pensions v Johnson* [2020] EWCA Civ 778 and *R (Pantellerisco) v Secretary of State for Work and Pensions* [2021] EWC Civ 1454.

[60] See N. Harris, *Law in a Complex State: Complexity in the Law and Structure of Welfare*, Oxford, Hart, 2013, 70-75.

[61] For example, there is an inter-active online process by which to "Check your State Pension" as well as make pension claim: see Department for Work and Pensions, *Annual Report and Accounts, 2021-22* (HC 193), London, DWP, 2022, 42. Online claiming is also possible for State Pensions Credit, which is a means-tested alternative to and top-up for the State Pension for persons who either do not qualify for the State Pensions (for example, because they have an insufficient record of insurance contributions) or qualify for additional support because their State Pension entitlement is at a very low level.

[62] DWP, *Annual Report and Accounts, 2021-22* (HC 193), London, DWP, 2022, 52.

[63] Cabinet Office Press Release, 'Digital by default proposed for government services', 23 November 2010; Cabinet Office, *Government Digital Strategy*, London, Cabinet Office, 2012; National Audit Office, *Digital Britain 2: Putting users at the heart of government's digital services* (HC 1048) (Session 2012-13), London, NAO, 2013. See also M. Lane Fox, *Directgov2010 and Beyond: Revolution not Evolution*, London, HM Government, 2010, at www.gov.uk/government/publications/directgov-2010-and-beyond-revolution-not-evolution-a-report-by-martha-lane-fox. http://publications.cabinetoffice.gov.uk/digital/strategy/government-digital-strategy.pdf.

noted above) – and those in low paid employment, was accompanied by an administrative emphasis on digital usage.[64] The phased introduction of UC over the past decade in place of a range of means-tested benefits and credits has been a complex process, subject to delays. But there has remained a significant focus on online claiming and digital interaction between claimants and the administrative authorities. The Government's early estimate was that by full implementation of UC 80 per cent of claims would be online.[65]

UC has been described as "the UK's first 'digital by design' benefit".[66] Recipients of UC will have an online account (or "journal") which is intended to enable them to "access information about their claim and their… payments, much like the options that online banking services currently offer" and to provide a medium for reporting any significant changes of circumstances affecting them.[67] The online account is intended to be the "primary channel" for claimant–DWP interactions,[68] including exchanges of messages.[69] A leading welfare rights organisation, the Child Poverty Action Group, has however provided evidence that the "informal nature" of this online journal, including "chat" functionality, contributes to the lack of clarity about decisions taken in relation to a claim, making it difficult for the claimant to understand them and use their right to challenge them.[70]

It has also been recognised that notwithstanding the claimed advantages of the online system, such as greater administrative efficiencies, potentially reduced scope for fraud and overpayment, and improved practical convenience for claimants,[71] there is a need to ensure that people who lack the capacity or resources to utilise digital services receive proper consideration and assistance.[72] Unfortunately, the help service for claimants who lack the necessary skills or resources to negotiate the digital interface is front-loaded, in the sense that it does not assist claimants once they have received their first payment of the benefit.[73] Moreover, there has been a failure to identify, on the system, vulnerable groups who tend to struggle with engagement with such a process, who include claimants with "digital illiteracy or digital access issues".[74] There is a route to access via face-to-face communication or the telephone, but as Griffiths says, "official policy is to maximise the use of the online journal".[75]

There is also an electronic route to submitting information for a PIP claim. The "Digital PIP2 Service" was first introduced in 2020 during and because of the Covid-19 pandemic, as a "clear, secure and quick application route… that did not require [claimants] to leave their homes".[76] The importance of having a digital service for PIP claims and their administration has increased significantly with the marked growth in the number of claims for this benefit, noted above. However, while a full online option for PIP claimants is due to be rolled out by the DWP in 2024 it is currently only at an early stage of development and it is not yet capable of dealing effectively with repeat claims due to the amount of manual intervention that is needed for them.[77]

[64] For background, see R. Griffiths, *Universal Credit and Automated Decision Making: A Case of the Digital Tail Wagging the Policy Dog?,* in *Social Policy and Society* (advanced online version), 2021, 1.
[65] House of Commons Work and Pensions Committee, *Universal Credit Implementation: Meeting the Needs of Vulnerable Claimants* (HC 576), London, The Stationery Office, 2012, par. 19.
[66] Griffiths n.64 above.
[67] DWP, *Universal Credit: welfare that works* (Cm 7957), London, The Stationery Office, 2010, ch 4 par. 8 and 9.
[68] DWP, *Digital Strategy*, London, DWP, 2012, par. 9.1.
[69] National Audit Office, *Universal Credit: Getting to first payment* (HC 376), London, NAO, 2020, par. 2.17.
[70] Child Poverty Action Group (CPAG), *Computer Says 'No!' Stage one: information provision*, London, CPAG, 2019, 7-8, at https://cpag.org.uk/policy-and-campaigns/computer-says-no-access-justice-and-digitalisation-universal-credit.
[71] See Griffiths, n. 64 above.
[72] See Social Security Advisory Committee, *The Implementation of Universal Credit and the Support Needs of Claimants* (Occ Paper no. 10), London, Social Security Advisory Committee, 2013, ch.4. On the difficulties experienced by some claimants, see Human Rights Watch, *Automated Hardship How the Tech-Driven Overhaul of the UK's Social Security System Worsens Poverty* (Report), 2020, at www.hrw.org/sites/default/files/media_2020/09/uk0920_web_0.pdf.
[73] Griffiths, n.64 above, 7.
[74] National Audit Office, *Universal Credit: Getting to first payment* (HC 376), London, NAO, 2020, par. 3.7.
[75] Griffiths, n. 64 above, 7.
[76] DWP, Digital PIP2 Service (staff guide), London, DWP, 2022, 1.
[77] As noted by the DWP in a response to a Freedom of Information request dated 24 November 2022 (posted at www.whatdotheyknow.com/request/901815/response/2175967/attach/7/Response%2090896%201.pdf?cookie_passthrough=1) which is reported by the Rightsnet website at https://www.rightsnet.org.uk/welfare-rights/news/item/dwp-confirms-that-it-is-no-longer-accepting-repeat-pip-claims-through-its-digital-pip2-service.

The development of the digital service forms part of the much wider 10 year Health Transformation Programme under which a "single digital platform developed by DWP" is to be established.[78] A joined up approach is planned involving DWP Digital and NHS Digital. DWP Digital, the DWP's digital development arm, is steering the Department's digital transformation. NHS Digital (established as the Health and Social Care Information Centre (HSCIC)) operates digital services for the National Health Service (NHS).[79] Unlike DWP Digital, NHS Digital was established by an Act of Parliament.[80] The joined-up approach will include the formation of a "service community", recognising for example that "People applying for benefits relating to their health may need to interact with a number of different departments including the NHS."[81] An aim of the integrated service is to bring health/disability assessments for a range of benefits, including PIP, "onto a single, digital system", enabling medical information relating to the claimant to be shared across departments (provided the claimant has given consent).[82] An online tool based on existing technology operated by NHS Digital is being developed to facilitate the sharing of the claimant's NHS health information with the DWP.[83] A small-scale implementation of this policy of establishing an integrated "Health Assessment Service" is already occurring, involving just a few areas, and it is aiming to be "user-friendly", enabling claimants of multiple health and disability benefits to submit evidence via a single route.[84] It is planned that evidence, including details of the claimant's health and disability over time, will be able to be presented and maintained in an online Health Input Record and could include input from social care support networks.[85] These developments are ground-breaking and could result in more accurate assessments although success is clearly dependent not only on technical reliability but also on claimants' capacity for interaction with the system and trust in its security.

3.2. *Health and disability benefits and the digital divide*

While chronic ill-health or disability can affect those of any age, the greatest prevalence is among older people. Consequently, social security benefits that are related to these circumstances are more likely to be received by older citizens. The fact that this age group has tended to experience greater barriers in accessing digital services than younger claimants[86]– an aspect of the 'digital divide' – is therefore particularly problematic. This is especially so in view of the UK Government's commitment towards the increased use of digital interfaces for disability benefits and long-term sickness benefits.[87]

There is evidence that some people with health or disability issues may prefer remote or online access to services.[88] But the digital divide has to be considered. Research has shown how someone with a disability who needs to engage with the social security system but lacks digital access is likely to have a reduced awareness of their entitlements, which in turn would impact on

[78] House of Commons Statement, Mr .J Tomlinson, Minister of State for Disabled People, Health and Work, 'Health Transformation Programme Update', 9 June 2020. See also Department for Work and Pensions, *Annual Report and Accounts, 2021-22* (HC 193), London, DWP, 2022, 40. For details of how the Programme will facilitate digital communication and interaction with claimants, see NAO, *Transforming health assessments for disability benefits* (HC 1512), London, NAO, 2023, Pt 2.

[79] It is an executive non-departmental public body. See the website https://digital.nhs.uk/ and see also NHS Digital, *Annual Report and Accounts 2021-22* (HC 795), Leeds, NHS Digital, 2022.

[80] Health and Social Care Act 2012, s.252 and Schedule 18. It has since been brought into NHS England (see the Health and Social Care Information Centre (Transfer of Functions, Abolition and Transitional Provisions) Regulations 2023 (SI 2023/98)). NHS England is the executive body steering the NHS in England.

[81] DWP Digital blog, Developing a health and benefits service community (posted 10 October 2019) at https://dwpdigital.blog.gov.uk/2019/10/10/developing-a-health-and-benefits-service-community/.

[82] DWP, *Shaping future support: the health and disability green paper*, London, DWP, 2021, par. 170. See also DWP, *Transforming Support: The Health and Disability White Paper* (CP 807), London, DWP, 2023, par. 120.

[83] DWP, *Transforming Support: The Health and Disability White Paper* (CP 807), London, DWP, 2023, par. 120-121.

[84] See Work and Pensions Committee, *Health assessments for benefits*, Fifth Report of Session 2022−23 (HC 128), London, House of Commons, 2023, par. 11 and 114.

[85] DWP (2023), n. 83 above, par. 123.

[86] National Audit Office, *Progress in making e-services accessible to all - encouraging use by older people,* London, The Stationery Office, 2003.

[87] DWP, *Shaping future support,* n. 82 above, par. 82, 110 and 150-151.

[88] *Ibid.*, par. 150.

the extent to which their needs are met.[89] Claimants are said to be "increasingly expected to access support via a digitalised system, in an environment where face-to-face advice provision and legal assistance has been greatly depleted", frustrating the efforts of the digitally excluded in seeking assistance[90] or redress.[91] Edmiston et al report that claimants with the most complex needs are the "most disadvantaged" by the withdrawal of such support services and "stand to lose out most from plans for further digitalisation in the benefits system beyond the pandemic".[92]

A major survey by the UK's Office for National Statistics, published in 2019, found that overall rates of digital access were increasing among people aged 65 or over, having nearly doubled between 2011−18.[93] For example, the proportion of people age 65-74 in the UK who had used the internet during the previous three months rose from 57.4 to 81.6 per cent (males) and 47.1 to 78.9 per cent (females) over this period.[94] Nevertheless, the over 65s still comprised around 80 per cent of all non-users of the internet (with more female non-users than male non-users).[95] Moreover, in terms of the future, the Office also predicted that although members of this age group were likely to be more digitally engaged than their predecessors, problems could arise:

> "For some, health problems as they age could lead to a decline in digital engagement, particularly if ageing impacts on cognitive ability. Technology may also change again so that the digital skills they have developed through their life will no longer be the skills that are needed."[96]

The Office considered that technological developments could, however, offset such difficulties, for example thorough voice-activated internet services and by ensuring that support is available for older people.[97] Nevertheless, recently a blind man brought a successful case in the High Court against the DWP for failing to ensure he had electronic communications which his software could read out, having instead sent him paper letters or PDF email attachments.[98]

Having a degree of digital competence may, in any event, be insufficient to manage a digital interface for claiming benefit. A survey in Northern Ireland found that one reason for not claiming Pension Credit − a means-tested benefit for people of state pension age, distinct from the state pension − was the lack of ability to complete claims online (although other application routes were available, including telephone claims). Moreover, most of those who did claim it, whether online or otherwise, were reliant on help with the process from a family or community member or a social worker.[99] Similarly, there is important evidence from a DWP-commissioned survey of UC claimants, who will be outside the older age group where digital capacity is less prevalent but will include significant numbers of people with vulnerabilities due to health problems − indeed, nearly one in three UC recipients have limited capability for work due to mental or physical ill health or disability.[100] It found that 43 per cent of the claimants needed additional help with registering their online account, 25 per cent were not able to submit their claim

[89] NatCen, *Uses of Health and Disability Benefits* (draft), London, DWP, 2022, 57, published online at https://committees.parliament.uk/publications/8745/documents/88599/default/. This draft report was sent to the House of Commons Work and Pensions Committee in January 2022 and was published online by the Committee (using Parliamentary powers following the DWP's refusal to publish it: see https://committees.parliament.uk/committee/164/work-and-pensions-committee/news/160255/work-and-pensions-committee-to-use-parliamentary-powers-to-publish-report-after-dwps-refusal/).

[90] M. Simpson, G. McKeever and C. Fitzpatrick, *Legal protection against destitution in the UK: the case for a right to a subsistence minimum*, in *Modern Law Review (online)*, (no vol. no.) 2022, 1-33, 23.

[91] P.W. Fay Henman, n. 58 above, 473.

[92] D. Edmiston *et al.*, *Mediating the claim? How "local ecosystems of support" shape the operation and experience of UK social security,* in *Social Policy & Administration*, vol. 56, no. 5, 2022, 775-790, 787.

[93] Office for National Statistics, *Exploring the UK's digital divide*, London, ONS, 2019), at www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/articles/exploringtheuksdigitaldivide/2019-03-04

[94] *Ibid.*, 12.

[95] *Ibid.*, 10-13.

[96] *Ibid.*, 13.

[97] *Ibid*.

[98] www.leighday.co.uk/news/news/2023-news/dwp-in-breach-of-equality-laws-after-failure-to-communicate-accessibly-with-blind-benefits-claimants/

[99] NISRA (Northern Ireland Statistics and Research Agency), *A Study on Factors that Enable or Constrain Take-Up of Pension Credit*, Belfast, Department for Communities (Northern Ireland), 2022, 11 and 64.

[100] DWP, Universal Credit Work Capability Assessment, April 2019 to December 2023 (2024) (at www.gov.uk/government/statistics/universal-credit-work-capability-assessment-statistics-april-2019-to-december-2023/universal-credit-work-capability-assessment-april-2019-to-december-2023).

online − "predominantly due to difficulties using or accessing computers or the internet" − and 31 per cent needed further help in managing their account.[101] It has also separately been reported that the more vulnerable groups, including those on long term sickness benefit, have had greater difficulty than others in coping with the online approach.[102] Additionally, a survey of child benefit claimants found that digital capability as regards claiming online was lower among those with health problems than for those without them.[103]

So, digital interfaces have a central role in the delivery of social security benefits and in interactions between benefit claimants and administrative operatives. Their use is continually extending across the social security system, including the parts of it providing health-related and disability-related benefits. Yet although some recipients of these benefits may prefer online processes and are content and able to use them, others potentially face the greatest barriers among all benefit claimants to accessing them. This difficulty may have a particularly pronounced effect when it comes to a key legal obligation on these claimants: to report changes in their circumstances.

4. *Changes of Circumstances and Underpayment or Overpayment of Benefit*

We have seen that entitlement to health or disability benefits is contingent upon an assessment of the claimant's mobility and/or their capacity to undertake various everyday activities or to self-care. Once an award is in place, any significant change to their condition that would affect an assessment of their needs, and therefore entitlement, ought to be taken into account by the administrative authorities so that an adjustment can be made if appropriate, usually via a "supersession" decision. The guidance to the public on reporting a change of circumstances is lacking in detail, although given their range, it would be difficult to list all of the potentially relevant circumstances precisely. On health and disability, the guidance adopts a very broad approach, simply advising the reporting of "any changes to your medical condition or disability".[104] Where an adjustment of benefit should have occurred in response to a relevant change in circumstances, but does not, there could be a resulting overpayment or underpayment.

4.1. *The contribution of claimant error to over/underpayment*

Overpayments and underpayments of benefit occur on a frequent basis within the UK social security system. Some result from administrative errors by the authorities. But a significant number arise from a failure by a claimant to notify the administrative authorities of a change in their condition or other circumstances. This failure could be due to fraud, which is a criminal offence and occurs when the claimant "dishonestly" fails to report a material change that he or she "knows… affects an entitlement of his to such a benefit or other payment or advantage".[105] The DWP is seeking to enhance the detection of fraud through the use of algorithms and "digital forensics".[106] Alternatively, over/underpayment could arise from a "claimant error", which is considered to have occurred when the claimant "has provided inaccurate or incomplete information, or failed to report a change in their circumstances, but there is no evidence of fraudulent intent on the claimant's part".[107] Therefore, it could be the result of the claimant's ignorance or inadvertent oversight. Indeed, research has shown that claimant ignorance or confusion has led to failures to appreciate the need to

[101] IFF Research, *Universal Credit Full Service Survey* (Research Report 958), London, DWP, 2018, par. 1.3.1.
[102] N Timmins, *Universal Credit: From disaster to recovery?* London, Institute for Government, 2016, 60.
[103] N Mitchell and L Adams, *Digital Child Benefit Customer Survey*, London, Her Majesty's Revenue and Customs (HMRC), 2022, par. 7.12.
[104] DWP, 'Benefits: report a change in your circumstances', at www.gov.uk/report-benefits-change-circumstances.
[105] Social Security Administration Act 1992, ss 111A and 112.
[106] Department for Work and Pensions, *Annual Report and Accounts, 2021-22* (HC 193), London, DWP, 2022, 73 and S. Trendall, *"A lack of transparency and accountability" – DWP urged to shed light on fraud algorithm*, publictechnology.net, 31 October 2022: www.publictechnology.net/articles/features/lack-transparency-and-accountability-%E2%80%93-dwp-urged-shed-light-fraud-algorithm (accessed 5 December 2022).
[107] DWP, Fraud and error in the benefit system Financial Year Ending (FYE) 2023 (May 2023) statistics, at www.gov.uk/government/statistics/fraud-and-error-in-the-benefit-system-financial-year-2022-to-2023-estimates/fraud-and-error-in-the-benefit-system-financial-year-ending-fye-2023#:~:text=Overpayments,The%20total%20rate%20of%20benefit%20expenditure%20overpaid%20in%20FYE%202023,was%20the%20highest%20recorded%20level.

report changes or the kinds of changes that matter for this purpose.[108] Fimister, for example, found that 40 per cent of benefit claimants lacked knowledge about the requirements on reporting changes.[109]

If an overpayment of benefit occurs due to a claimant's failure to disclose to the appropriate office a "material fact", meaning some fact potentially having a bearing on entitlement under a benefit award,[110] any overpaid benefit will be recoverable from the claimant.[111] The recovery is usually made via deductions from monthly payments.[112] Recent estimated annual overpayment and underpayment rates and their cause are set out in Table 1. The rates shown represent the total proportion of benefit that was either not paid when there was entitlement to it (underpayment) or was wrongly paid due to fraud or error (overpayment), as a proportion of actual total benefit expenditure.

Overpayments		Underpayments	
Fraud	*2.7%*		-
Claimant error	*0.6%*	Claimant error	*0.9%*
Official error	*0.3%*	Official error	*0.5%*
Total overpaid	*3.6%*	Total underpaid	*1.4%*

Table 1: Estimated Overpayment and Underpayment Rates for Social Security Benefits in Great Britain, Year to April 2023[113]

It is significant that in the case of one benefit, AA, the chief cause of underpayment in 2022 was when the claimant's disability had "deteriorated and/or their care needs have increased enough to change the rate they are eligible for, but they do not inform the Department and are therefore paid at the lower rate rather than higher rate (of the benefit)".[114] Indeed, almost all of the AA underpayments arose from claimant error rather than official error. They totalled £200 million in the year ending 2022.[115]

Underpayments of PIP totalled £900 million in 2023 of which £840 million was due to claimant error; and the DWP reports that *all* of these claimant error underpayments resulted from "errors where the claimant's condition had got worse and they failed to inform the department".[116]

These figures underline the significance of changes of circumstances (particularly concerning health) in relation to benefit awards and the importance of ensuring effective communication of them.

4.2. *The obligation to report changes of circumstances*

4.2.1. *The nature of the claimant's duty*

The claimant has an obligation, set out in regulations, to notify the Secretary of State (in reality this means the DWP) of "any change of circumstances" which the claimant "might reasonably be expected to know might affect" either the continuance of entitlement to benefit, the amount of benefit or the payment of benefit, and to do so "as soon as reasonably practicable after the change occurs".[117] The duty applies even if the award was made for a fixed period. Many awards of PIP, for example, are fixed term, on the assumption that there could be changes in the claimant's disabling condition and therefore their needs beyond the set period. Just over three-quarters of PIP recipients are on fixed period awards of

[108] See G. Fimister, *Reporting changes in circumstances: factors affecting the behaviours of benefit claimants*, DWP Research Report No. 544, London, DWP, 2009; A. Irvine, J. Davidson and R. Sainsbury, *Reporting Changes in Circumstances: Tackling Error in the Benefits System*, DWP Research Report No. 497, London, DWP, 2008; M. Boath and H. Wilkinson, *Achieving good reporting of changes in circumstances*, DWP Research Report No. 457, Leeds, Corporate Document Services, 2007.

[109] *Ibid*.

[110] See Social Security Commissioner's Decision *R(IS)9/06*.

[111] Social Security Administration Act 1992, s.71.

[112] See R. Griffiths and R. Cain, *Universal Credit, deductions and "sexually transmitted" debt* in *Journal of Social Welfare and Family Law* (advanced online publication), 2022, 1-24, at 7-8.

[113] DWP (2023), n. 107 above.

[114] *Ibid*. The reference to 'higher rate' refers to the fact that the claimant receives the lower rate of benefit, paid to those with lesser care needs, rather than the higher rate paid to those with more significant needs. Comparable information on AA is not available for 2023.

[115] DWP, Fraud and error in the benefit system Financial Year Ending (FYE) 2022 (May 2022) statistics, at www.gov.uk/government/statistics/fraud-and-error-in-the-benefit-system-financial-year-2021-to-2022-estimates/fraud-and-error-in-the-benefit-system-financial-year-ending-fye-2022

[116] DWP (2023) n. 107 above.

[117] The Social Security (Claims and Payments) Regulations 1987 (SI 1987/1968) (the 1987 Regulations), reg.32(1B) and the Universal Credit, Personal Independence Payment, Jobseeker's Allowance and Employment and Support Allowance (Claims and Payments) Regulations 2013 (SI 2013/380) (the 2013 Regulations), reg.38(4). Note that this is distinct from separate duties to provide information or evidence required by the DWP in connection with a claim; in that context the reasonableness in relation to the claimant's knowledge is irrelevant.

two years or less.[118] Nevertheless, any change prior to the expiry of the fixed period needs to be reported. For long-standing or indefinite awards there is no scheduled (re-)assessment until a "light touch" assessment after 10 years,[119] so self-reporting any change in the interim will be particularly important.

In addition to this duty to notify a change of circumstances there is a more general duty to provide "in such manner and at such times as the Secretary of State may determine such information or evidence as the Secretary of State may require in connection with payment of the benefit claimed or awarded".[120] However, this duty and the change of circumstances duty are considered to be linked,[121] in the sense that the duty to provide any relevant information to the Department is an ongoing one during the continuance of the award.

Case law makes clear that a claimant is not necessarily expected to report undramatic changes in health or disability that have occurred over a prolonged period.[122] An award could have started many years ago and it has been held judicially that it would not be reasonable to expect the claimant to remember their precise condition far in the past and be able to make a comparison between then and the present. Instead, they need only to compare their present and their earlier condition over a "reasonable time frame", a period sufficient "to show overall a sustained improvement or deterioration, taking account of any usual variation".[123]

It has also been held that the instructions in the official notes sent by the DWP to benefit recipients have a bearing on whether a claimant should realise the need to report a change, although what it is reasonable for the claimant to know in any individual case might hinge on their mental state and other relevant factors.[124] In one case the notes had stated:

"We need to know if anything you told us changes about how your illness or disability affects you. Please tell us if things get easier or more difficult for you. And tell us if you need more or less help."[125]

It seems probable that any person who has received such notes and has benefited from a hip operation in the way the claimant in this particular case had done, by experiencing an improvement in walking ability, would be expected to know that they should report the change. Furthermore, it has since been held by the Court of Appeal, in *B v Secretary of State for Work and Pensions*, that an overpayment of benefit resulting from a failure to disclose a material fact of which the claimant was aware (in this case, that the claimant's children had been taken into local authority care) is recoverable by the authorities even if the claimant did not actually appreciate that reporting of it was necessary.[126] The test of whether it is "reasonable" to know that the change might affect one's entitlement to benefit, in other words whether the change is a material fact, was considered an objective rather than a subjective one.[127]

This approach was subsequently held by the European Court of Human Rights to be consistent with the European Convention on Human Rights, in *B v United Kingdom*, which involved the same claimant. The complaint was of discrimination contrary to Article 14 read with Article 1 of the First Protocol, arguing that claimants who could not reasonably be expected to report a material fact because of being *unaware of that fact* were treated differently to claimants who could not reasonably be expected to report the fact because they were *unaware of the requirement to report* it. Were the two groups of claimants in an analogous situation, on the basis that neither of them could reasonably be expected to report the relevant fact and they were equally blameless for not doing so? The Court decided that they were *not* analogous situations. The situation where someone was not aware of a fact was "qualitatively of a different nature" to where someone was

[118] See PIP statistics cited in n.1. above. The law requires PIP awards to be fixed term unless that is considered "inappropriate": Welfare Reform Act 2012 s.88.
[119] See DWP, The Personal Independence Payment (PIP) toolkit, at www.gov.uk/guidance/the-personal-independence-payment-pip-toolkit.
[120] 1987 Regulations above, reg. 32(1A). See also the 2013 Regulations, reg. 38(3).
[121] Commissioner's Decision *CDLA/2328/2006*, a decision of a Social Security and Child Support Commissioner. The functions of the Commissioners, to hear appeals from decisions of first-tier tribunals, was transferred to a new Upper Tribunal in 2008 under the Tribunals, Courts and Enforcement Act 2007.
[122] *Ibid*.
[123] *Ibid.*, par. 24.
[124] *Ibid.*, par. 28.
[125] *Ibid.*, noted at par. 18.
[126] *B v Secretary of State for Work and Pensions* [2005] EWCA Civ 929.
[127] *Ibid.*, par. [40].

"aware of a fact but… not aware of its materiality": the latter but not the former depended on "difficult questions of cognitive capacity and moral sensitivity which vary from person to person".[128]

The claimant's alternative argument in *B v United Kingdom* was that because she was incapable of understanding that she should report a material fact to the Department she should have been treated differently from someone who had such a capability. However, the Court said that the difference in treatment was in pursuit of a legitimate aim, "namely that of ensuring the smooth operation of the welfare system and the facilitation of the recovery of overpaid benefits", and was "objectively and reasonably justified", since requiring decision-makers to assess the claimant's understanding or mental capacity for this purpose would hinder recovery of overpaid benefit and reduce public resources.[129] The treatment was also considered proportional in that it was accepted that public authorities have the right to correct errors in the award of benefits provided an excessive burden is not placed on the individual (here the mitigation was that repayment was by monthly instalments) and the claimant had not requested a waiver of the recovery of the overpaid benefit on the basis that such recovery would be detrimental to the claimant's health or welfare.[130]

So, the requirement to report a change of circumstances, such as a material change in a medical condition or disability, is likely to be treated strictly. If digital access can improve the claimant's ability to fulfil this requirement it would be particularly beneficial. Alternative means of reporting would need to be permitted, however, since otherwise there might be grounds for an Article 14 claim on the basis that those lacking mental or physical capacity for online engagement are unjustifiably disadvantaged compared with others. Leaving this aside, the fall in the reporting of changes of circumstance during the Covid-19 pandemic, in the case of PIP,[131] for which digital usage is still nowhere near normative, demonstrates why digital communication can make a difference to claimant engagement with the benefit system for such purposes.

4.2.2. *Using digital technology to report changes successfully*

Social security law permits the communication of information or evidence relating to a change of circumstances to be undertaken by the claimant electronically provided various conditions are met.[132] Essentially, this form of communication must have been officially approved and comprise online communication using the official route. Where the approved method is not used, the information provided will be treated as not having been submitted.[133] Using an unapproved method (for example, a simple email) might, therefore, result in the information not being classed as officially received and disclosed to the DWP, leading to a potential overpayment of benefit which could be recoverable from the claimant. The online facility is particularly relevant to UC claims, as described earlier, and the lack of progress in making this route more widely open across different benefits (for example, contributory ESA recipients must report changes via the telephone or postal services[134]) is regrettable.

A problem that has emerged in relation to UC is that third parties who are supporting claimants do not have direct access to the UC online journal which, as noted earlier, is intended to be the principal channel of communication for reporting changes of circumstances as well as for other interactions. Someone representing an ill or vulnerable claimant might therefore be hampered in their efforts to keep the Department informed of relevant matters. The National Audit Office has recommended allowing claimants' supporters access to a version of the journal to enable them to "view appropriate shared information and communicate with the Department".[135]

[128] *B v the United Kingdom* (Appl. No. 36571/06) [2012] ECHR 255, par. [57].
[129] *Ibid.*, par. [59] and [62].
[130] *Ibid.*, par. [60]-[61].
[131] DWP, Official Statistics: Personal Independence Payment: Official Statistics to April 2022 (published 2022), at www.gov.uk/government/statistics/personal-independence-payment-statistics-to-april-2022/personal-independence-payment-official-statistics-to-april-2022.
[132] 1987 Regulations, reg.32ZA and Schedule 9ZC; 2013 Regulations, Schedule 2.
[133] See the 1987 Regulations, Schedule 2 par. 2; and the 2013 Regulations, Schedule 2 par. 2.
[134] As advised by the DWP in its detailed guidance for claimants at www.gov.uk/guidance/new-style-employment-and-support-allowance-detailed-guide.
[135] National Audit Office (NAO), *Rolling Out Universal Credit* (HC 1123) (Session 2017-2019), London, NAO, 2018, par. 19. The NAO is an agency tasked with

The benefits to the claimant of electronic communication via digital channels for reporting a change of circumstances include the relative certainty, provided the system works properly, that the DWP will receive the relevant information and be able to act upon it where appropriate. In any event, it should also provide a probative electronic footprint relating to the sending or uploading of the information. There is, however, a question over whether it may also potentially avoid the difficulty faced by some claimants in ensuring that the information is correctly channelled to the relevant DWP office or section. For example, a claimant receiving more than one social security benefit may assume (not necessarily correctly) that a communication to just *one* of the offices handling the different awards may satisfy the obligation to notify a change of circumstances. The law, however, requires the change of circumstances notification relevant to an individual benefit to be given to the "appropriate office" (in writing or, unless specifically required to be given in writing, by telephone).[136]

This issue was highlighted in an inquiry by the House of Commons Work and Pensions Committee into overpayment of Carer's Allowance paid (as noted above) to people who provide substantial care for another person who receives disability benefit. In its report, the Committee noted that the DWP, in an annual reminder to recipients, states that their Carer's Allowance entitlement "could be affected" if there is a change in their circumstances. The reminder also provides an internet link for reporting any such change to the relevant administrative office, the "CA Unit". However, the Committee criticises the Department for not also making clear to recipients that changes of circumstances *must* be reported *directly* to the Unit "even if claimants have reported the changes to other DWP departments who may need to be informed". [137] A claimant would be wrong to assume that the different offices or sections are all joined up administratively, particularly through an IT system, so that informing one part of the system might be sufficient. This has long been an aspect of the complexity of the social security system that claimants find particularly problematic.[138] It has been exacerbated by the only partial linking of different agencies' computer systems.[139] Although the replacement of six separate benefits by UC has led to a more unified system than previously existed, the migration of claimants from the benefits that are being replaced has been a greatly protracted one and is still not complete.

The problem of failing to report changes to the "appropriate office" was highlighted in an important case in 2005: *Hinchy v Secretary of State for Social Security*.[140] The claimant received a disability premium in her social assistance benefit (Income Support). Her entitlement to this premium was triggered by her receipt of the DLA care component at the middle rate. When her DLA award ended, payment of her disability premium should therefore also have stopped. However, the premium wrongly continued in payment, because the Income Support office was unaware the DLA award had ended. A total of £3,500 in disability premium was overpaid and the Secretary of State sought to recover it.[141] The claimant appealed, but the first-tier tribunal rejected her claim to have conveyed the information by telephone, since there was no record of her call. The tribunal also considered it clear from the notice printed in her Income Support order book that it was important for her to notify the appropriate office of relevant changes. The tribunal concluded that it was reasonable to expect her to have read the instructions. Also, the case law confirmed that she was under an

providing arms-length scrutiny of government economic efficiency in service provision.

[136] See, for example, the 2013 Regulations, reg.38(5).

[137] House of Commons Work and Pensions Committee, *Overpayments of Carer's Allowance* (Session 2017-19) (HC 1772), London, House of Commons, 2019.

[138] House of Commons Work and Pensions Committee, *Benefits Simplification, Vol.1* (HC 463-I), London, The Stationery Office, 2007, par. 10.

[139] NAO, *Department for Work and Pensions: Dealing with the Complexity of the Benefits System*, London, NAO, 2005, par. 2.24. The problematic situation described by Henman and Adler over 20 years ago, of a frequent absence of an automatic flow of information between different benefit administrations (P. Herman and M. Adler, *Information technology and transformation in social security policy and administration: A review*, in *International Social Security Review*, 54, No. 4, 2001 23-49, 30), has still not been fully redressed. For a recent example, see *WS v Secretary of State for Work and Pensions* [2023] UKUT 81 (AAC) (DWP and HMRC were linked by a RTI (real time information) feed but this did not mean that a claimant's reported change of circumstances was known to both).

[140] [2005] UKHL 16.

[141] Under the Social Security Administration Act 1971, s 71(1).

obligation to provide any relevant information to the appropriate office.

The case progressed to the Court of Appeal, which concluded that the information relating to the ending of the DLA award did *not* need to be communicated to the Income Support office as the fact was already known to the DLA officials and it was reasonable for the claimant to believe that other benefit officials would be aware of it. When the case was subsequently heard in the House of Lords, one of the judges, Lord Scott, in effect blamed the DWP for not ensuring that the instructions in the order book were clear about having to inform a specific office about the ending of the DLA award.[142] However, the other four judges took a hard line. Lord Hoffmann said that there was an onus on the claimant to report changes appropriately and the relevant official could not be deemed to know something that was actually unknown to them.[143] Although Baroness Hale expressed doubts about the clarity of the order book's instructions in informing the claimant of her obligations,[144] the question of whether claimant ought reasonably to have known that she was obliged to report the termination of her DLA award was a matter to be left to the first-tier tribunal's judgment.[145]

The *Hinchy* case therefore reinforced the burden on claimants in trying to manage with the complexities of the social security system, while it also highlighted the system's disparateness and lack of cohesion, factors which have in fact made the employment of joined-up digital processes both more necessary but at the same time more difficult.[146]

In addition to a disjunction between different computer systems, there is also the problem where individual systems do not work efficiently. In one case[147] the claimant had informed the Department by telephone of a change of circumstances and was informed that the system was "down" and they would contact her again, which did not happen. As her benefit was not adjusted, she was overpaid a significant sum, a total of £11,000. The DWP argued that she had a continuing obligation to disclose her circumstances, with the implication that she should have persisted with informing them until the adjustment to her benefit was made. However, Upper Tribunal Judge Wikeley held that the claimant had met her disclosure obligation when she telephoned with the information. Claimants of most social security benefits in the UK, including disability benefits, are advised by the DWP to telephone in details of changes of circumstances, the exception being UC claimants, who as noted above will normally be expected to use their online account.[148] However, the danger that the information may not be recorded will normally make the online route seem much safer and more reliable from a claimant's perspective.

5. *Conclusion*

In the light of the large numbers of UK citizens currently eligible for and receiving sickness or disability benefits (nearly half of the total recipients across these categories are receiving both types[149]) it is not surprising that the Government's ongoing digitalisation programme for social security is having an increasingly marked impact on these particularly disadvantaged and vulnerable claimants. Interaction by digital means between the administrative authorities and claimants is a particular feature of this new emphasis within social security administration. There is an expectation by the policy makers that the normative status of digital communication for claims and the management of awards, including decisions and adjustments, will become firmly entrenched within this area of social security as it is in the context of mainstream out-of-work benefits. However, it is important that account is taken of the Work and Pensions Committee's recent warning in relation to health and disability benefits that "digital does

[142] [2005] UKHL 16 at par. 46 (Lord Scott of Foscote).
[143] *Ibid*. at par. 32 (Lord Hoffmann). This situation may be contrasted with that in a Commissioner's case (*CIS/1887/2002*) in which the claimant's Income Support was overpaid because his payments were not adjusted to take account of his simultaneous award of Incapacity Benefit but it was held that the administrative office for Income Support was the same office as the one that handled Incapacity Benefit and should therefore have known about the latter award.
[144] *Hinchy* n. 142 above, par. 57.
[145] *Ibid.* at par. 58.
[146] See for example the comments by the chair of the Committee in Social Security Advisory Committee, *Seventeenth Report, 2004*, Leeds, Corporate Document Services, 2004, foreword.
[147] *CIS/3529/2008* [2009] UKUT 52 (UT).
[148] See the statement at www.gov.uk/report-benefits-change-circumstances.
[149] DWP (2023) n. 82 above, par. 139.

not work for everyone" and its recommendation that "alongside the digital platform" there need to be "alternative formats and channels… easily available to those who need them".[150] Digital will nevertheless be the default and given this expectation it is ironic that mental or physical problems that affect a person's digital capacity may, as we have seen, be relevant factors in the assessment of their entitlement to the health-related and disability-related benefits. This is unlikely to change even if the Work Capability Assessment is reformed or replaced, as is expected to occur, following the publication of proposals by the Government in March and November 2023.[151]

One of the most important aspects of the two-way information flow by digital means between the provider and the recipient of benefit relates to the obligation on the latter to report to the former any change of personal circumstances relating to health and disability insofar as it relates to and affects their physical or mental capacity for work or to self-care or mobilise. The strictness of the rules is underlined by the case law. As we have seen, this is a problematic issue since failures to report such changes can result in underpayment of benefit or to an accumulation of overpaid benefit that will need to be repaid by the claimant, with the attendant risk of hardship. It is important that any barriers to the correct reporting of changes, which is not always a straightforward matter for claimants, are minimised. To this end, further measures and support will be needed to bridge digital the divide which clearly disadvantages some disabled and long-term sick claimants disproportionately.

[150] See Work and Pensions Committee, *Health assessments for benefits*, Fifth Report of Session 2022−23 (HC 128, London, House of Commons, 2023, par. 61.

[151] DWP (2023) n.82 above, Chapter 4 and *Government Response to the Work Capability Assessment: Activities and Descriptors Consultation* (CP 973), London, DWP, 2023. Those receiving a disability benefit would qualify for UC limited capability (to be renamed "UC health element") without the need for a separate health (WCA) assessment, whereas those not receiving a disability benefit would not undergo a WCA either but would in effect be assessed under the PIP criteria but will also be subjected to a new "personalised health conditionality approach". Much more detail (and new legislation) relating to the proposals will be needed, but if approved the reform would be rolled out from 2026/27. For analysis of potential impact, see Resolution Foundation (RF), *Reassessing the Work Capability Assessment* (RF, 2023), at www.resolutionfoundation.org/publications /reassessing-the-work-capability-assessment/. See also S R Chaudhuri and T Waters, *The effects of reforms to the Work Capability Assessment for incapacity benefits*, London, Institute for Fiscal Studies, 2023.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 267-272
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 21

*The Cybersecurity of Health Data Hosted by Public Administrations**

Marcel Moritz
(Senior public-law lecturer at University of Lille, France CERAPS UMR8026)

ABSTRACT As cyber-attacks on health data increase, securing health data is a growing challenge. But this security is not only a mere technical issue aimed at preventing malicious third parties. It is also necessary to ensure the legal security of the chosen hosting solutions, in the context of the opening up of health data, which itself raises many questions. These are the challenges that need to be resolved in order to give full effect to the perspectives offered by the massive processing of these data.

1. *Introduction*

Health data[1] are considered sensitive data within the meaning of the General Data Protection Regulation (GDPR),[2] and as such must benefit from special protection. Indeed, the information likely to be revealed by these data generates particularly serious risks. In wrong hands, these data could, for example, limit access to certain services, or make it difficult to obtain a loan or a job. It is therefore not surprising that health data are one of the most widely traded data on the Darknet.[3] Their value is often far greater than that of bank-card data. The processing of such data therefore requires trust in the controller, especially when the latter is a public administration, such as a hospital, processing large amounts of data. Legally, the GDPR provides several general privacy guarantees for the processing of health data. For example, most processing of such data requires a privacy-impact assessment to be carried out beforehand, as well as the appointment of a data-protection officer. These safeguards are further increased in the context of processing by public administrations, since the latter are always subject to the obligation to appoint a data-protection officer, even if the processing of health data does not take place on a large scale.

The question is whether these guarantees are sufficient, given the legitimate citizens' expectations regarding public bodies processing their health data. From our point of view, this is not a mere matter of personal-data security, but an essential condition for maintaining the public's trust in the State and its public services. To put it another way, in view of the risks and the legitimate trust that citizens are supposed to have in the public administration, the latter's processing of health data should be perfectly irreproachable in terms of technical, organisational, and legal security. However, many recent examples show that this information-security management is not fully satisfying. To give just one example that has received considerable media coverage in France and beyond, we can mention the theft from Paris hospitals, in the summer of 2021, of the personal data of around 1.4 million people tested for Covid-19. This data breach was widely publicised, as required by the GDPR, which imposes communication to data subjects in such cases.[4] Thus, cybercrime has become a major issue for health data, which we will highlight in the first part. But there is also another important issue, that of the sovereignty of data storage and the legal risks induced by some cloud solutions. This will be developed in the second part. Finally, we would like to emphasise the risks induced by the future implementation of the data-governance act, in that it promotes open data, particularly personal and sometimes health data, which could well give rise to new legal

* Article submitted to double-blind peer review.

[1] Art. 4 §15 GDPR provides that: *"'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status"*.

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[3] www.keepersecurity.com/fr_FR/how-much-is-my-information-worth-to-hacker-dark-web.html.

[4] Indeed, according to art. 34 GDPR "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay".

risks. These aspects will be studied in the third part.

2. *Threats related to cybercrime and legal responses*

Unsurprisingly, cybercriminal groups are interested in health data because of their high value. Indeed, they can potentially be used for a variety of malicious purposes: phishing, ransomware,[5] advertising fake medicines, restricting access to bank credit or to certain services such as health insurance, training of artificial intelligence, etc. In the US, it was found that the annual number of ransomware attacks on health-care delivery organizations more than doubled from 2016 to 2021, exposing personal-health information of nearly 42 million patients.[6] In France, according to a May-2021 report,[7] in 2020, no fewer than 27 attacks affected French hospitals, and the health sector has suffered one cyberattack per week since the beginning of 2021. Even more worrying is the fact that these figures appear, according to the public authorities themselves, to be lower than reality: "Symptomatic of this disparity in the perception of the issues, the number of serious incidents reported by health establishments is still low and lower than the estimated reality".[8]

The general principles of the GDPR regarding data security impose de facto an enhanced protection for health data. Indeed, by advocating a risk-based approach, Article 32 imposes appropriate technical and organisational measures adapted to the risks[9], including for example "(a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing". This involves a risk-assessment carried out under the responsibility of the controller. The latter must also inform the competent data-protection authority in the case of personal-data breaches[10] and, "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons",[11] "communicate the personal data breach to the data subject without undue delay".[12] This is the reason why in the above-mentioned case of the theft of Covid-test data, a specific communication was set up after notification to the French Commission Nationale de l'Informatique et des Libertés (CNIL).[13]

In the case of health data, specific sectoral guidelines may apply, in particular the security guidelines resulting from the Politique Générale de Sécurité des Systèmes d'Information de Santé (General Policy on the Security of Health Information Systems) known as the PGSSI-S,[14] referred to in Articles L. 1470-5 and L. 1470-6 of the French Public Health Code (Code de la santé publique, CSP), as well as the Health data hosts (Hébergeur de données de santé, HDS) accreditation and certification guidelines, referred to in Article L. 1111-8 of the same Code. CNIL declaration or authorisation requirements may also apply,[15] for example the declaration of compliance with the reference methodology MR-003 applicable to health research without consent.[16]

But the most important security factor is probably that many health data are processed by stakeholders who are operators of essential

[5] In October 2020, at least 2,000 Finnish patients received an email threatening to publish the details of their psychological treatment on the web if they did not pay several hundred euros, after the data of a network of psychotherapy centres was hacked (www.slate.fr/story/215763/bonnes-feuilles-ma-sante-mes-donnees-coralie-lemke-premier-parallele-securite-gafam-secret-medical-informations).

[6] Vv. Aa., *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021*, in www.jamanetwork.com/journals/jama-health-forum/fullarticle/2799961.

[7] Ministère des solidarités et de la santé, *Cybersécurité dans le secteur de la santé et du médico-social : une priorité nationale pour réussir la transformation numérique*, dossier d'information, 05/2021, 28.

[8] *Ibid.*, 7.

[9] "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (...)".

[10] GDPR, art. 33.

[11] GDPR, art. 34.

[12] *Ibid.*

[13] www.cnil.fr/fr/fuite-de-donnees-de-sante-ap-hp-que-pouvez-vous-faire-si-vous-etes-concerne.

[14] www.esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire.

[15] www.cnil.fr/fr/declarer-un-fichier.

[16] www.cnil.fr/fr/declaration/mr-003-recherches-dans-le-domaine-de-la-sante-sans-recueil-du-consentement

services' and/or - under French law - operators of vital importance[17] - and are thus covered by the network and information system (NIS) Directive[18] and/or article 22 of the French law of 18 December 2013.[19] As a result of these texts, the entities concerned have an active obligation to implement certain cybersecurity measures under threat of sanctions and may be required to undergo control audits, carried out in France by the "Agence nationale de la sécurité des systèmes d'information" (ANSSI)[20] or by entities approved by this agency. These cybersecurity requirements apply to an increasing number of entities. For instance, on 22 February 2021, the Ministry of Solidarity and Health presented, via a press release, its ambitions in terms of IT security for hospitals and announced that 135 territorial hospital groupments[21] will be included in the list of operators of essential services. At the same time, it was announced that a budget of 350 million euros will be earmarked for strengthening the IT security of French health institutions. Aware of the limits of a repressive policy towards cyber criminals, public authorities have therefore focused in recent years on the development of cyber-security measures and the allocation of resources in this respect. However, this security can still be improved in many respects. The news has given us several mediatised examples, such as the cyber-attack by ransomware which targeted the Corbeil-Essonnes hospital in August 2022 and which led to the disclosure of data by the hackers. According to the institution, the data that was disseminated potentially include "certain administrative data", including the national insurance number, and "certain health data such as examination reports and in particular external anatomocytopathology, radiology, analysis laboratories and doctors' files".[22]

Moreover, it is not only a question of technical security, in the context of risks of criminal cyber-attacks, but also of guaranteeing the legal security of data hosted in the cloud. In many respects, this issue is at least as challenging.

3. *Threats related to data storage and legal responses*

The idea of keeping health data for study purposes, particularly statistical ones, is not new. As early as the 1980s, the Programme de médicalisation des systèmes d'information (PMSI) was created in France to provide a synthetic and standardised description of the medical activity of health establishments. Since then, many databases have been developed, in particular the hospital health-data warehouses (entrepôts de données de santé hospitaliers, EDSH)[23] to collect large amounts of data. The implementation of EDHSs in France dates back to the end of the 2000s and was reinforced at the end of the 2010s. There are about twenty warehouses, some of which have teams of several dozen full-time equivalent employees, while others are much more modest in terms of resources. The nature of the data processed also varies widely depending on the ESDH.[24] In addition to these warehouses, the law of 26 January 2016[25] gave birth to the National Health Data System (SNDS), to create one of the largest health databases in the world.

Managed by the National Health Insurance Fund (Caisse nationale de l'Assurance Maladie, CNAM), the SNDS contains (i) health insurance data, (ii) hospital data, (iii) databases on medical causes of death and (iv) data on disability. The 2019 law on the organisation and transformation of the healthcare system extended the scope of the SNDS to data for healthcare professionals and organisations, data on loss of autonomy, and surveys in the field of health, school medicine, maternal and child protection and labour medicine. The SNDS thus makes it possible to provide a complete vision of the care pathways of the entire French population, over

[17] "Opérateur d'importance vitale".
[18] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
[19] Law no. 2013-1168 of 18 December 2013 on military programming for the years 2014 to 2019 and on various provisions relating to defence and national security.
[20] www.ssi.gouv.fr.
[21] www.usine-digitale.fr/article/voici-la-strategie-gouvernementale-pour-lutter-contre-les-cyberattaques-contreles-hopitaux.N1063569
[22] www.lemonde.fr/pixels/article/2022/09/25/cybercriminalite-l-hopital-de-corbeil-essonnes-refuse-de-payer-la-rancon-les-hackeurs-ont-commence-a-diffuser-des-donnees_6143112_4408996.html.
[23] For a recent report regarding these warehouses: www.has-sante.fr/upload/docs/application/pdf/2022-11/rapport_entrepots_donnes_sante_hospitaliers.pdf.
[24] www.has-sante.fr/jcms/p_3386123/fr/entrepots-de-donnees-de-sante-hospitaliers-en-france.
[25] Law no. 2016-41 du 26 janv. 2016 for the modernisation of French healthcare system.

a maximum historical depth of 20 years[26], to improve health policies, healthcare provision, social protection, medic-social care and research, but also to enhance France's international competitiveness through the release of these data[27].

Since 2019, a Health Data Hub[28] (HDH) has been added to this set. This platform is intended to facilitate the sharing of health data from a wide variety of sources in order to promote research, especially in the field of artificial intelligence[29]. Shortly after its creation, a decision motivated by the pandemic broadened the scope of the data that can be processed[30].

If the HDH has caused such a stir in France, it is not so much because of the extent of the data likely to be shared, but because of the choice of its technical operator: Microsoft Azure. Indeed, as an American company, this corporation is subject to a legislation that may, in certain situations, require it to transmit data to the American authorities. For the record, the Court of Justice of the European Union (CJEU), in its judgment of 16 July 2020, known as "Schrems II", ruled that the surveillance carried out by the American intelligence services on the personal data of European citizens was excessive, insufficiently regulated and without any real possibility of appeal. It concluded that transfers of personal data from the European Union to the United States are contrary to the GDPR and the Charter of Fundamental Rights of the European Union, unless additional measures are put in place or the transfers are justified under Article 49 of the GDPR[31]. In the case of the HDH, the situation is somewhat different since the data are not transferred to the United States, but to an American company while remaining hosted in Europe, a point on which the Court did not rule directly in the Schrems II case. It is this state of affairs that led the French Conseil d'Etat to validate - at least in the current context - the contract between the French State and Microsoft Azure, while acknowledging that there is a risk that Microsoft could be forced to provide data to the US authorities[32]. In another judgment, it was judged that the fact that Microsoft is governed by US law and may have to transfer data to the United States for the administration of the technical solution it offers, "in accordance with the Commission's decision of 12 July 2016", cannot be considered, at the date of this order and in the state of the investigation, a seriously and manifestly unlawful interference with the fundamental freedoms that the GDPR is intended to protect[33].

The HDH has thus been at least temporarily saved. But the legal risks remain real, as the CNIL has consistently stated,[34] and will probably not be completely removed by the presidential decree signed by President Biden, directing the steps that the United States will take to implement U.S. commitments under the European Union-U.S. Data Privacy Framework[35].

The above-mentioned disputes are therefore probably not the last. They have had the essential merit of putting the need for a sovereign cloud back at the heart of the debate, particularly regarding health data. Thus, on 19 November 2020, the Minister of Health, Olivier Véran, sent a letter to the President of the CNIL, in which the Minister undertook to terminate the contract with Microsoft and transfer the hosting of the Health Data Hub to a French or European player within two years.[36] Almost three years

[26] www.assurance-maladie.ameli.fr/etudes-et-donnees/en-savoir-plus-snds/presentation-systeme-national-donnees-sante-snds.

[27] L. Cluzel-Métayer, *Les données de santé, ou le défi d'un partage sous haute protection*, in *Revue de droit sanitaire et social* (RDSS), 2022, 149.

[28] To note that the French State has been ordered to stop using the expression "Health Data Hub" and its acronym "HDH", since there are translations approved by the commission for the enrichment of the French language, Tribunal administratif de Paris, 20 October 2022, *Revue Lamy Droit de l'Immatériel* (RLDI), 197, 1 November 2022.

[29] For more details, see article L. 1462-1 Code de la santé publique.

[30] Judgment 21 April 2020.

[31] For a global analysis of the HDH with regard to GDPR, see www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub.

[32] Conseil d'État, ordonnance de référés, 13 October 2020, no. 444937: *La semaine juridique édition générale* (JCP G), 2020. 1358, comm. B. Bertrand ; *Revue Lamy droit de l'immatériel,* 2020, 176, 5974, comm. P. Navarro and F. Zannotti.

[33] Conseil d'État, ordonnance de référés, 19 June 2020, n° 440916, pt. 28 : *Revue Lamy droit de l'immatériel* (RLDI) 2020/172, n° 5904, obs. L. Costes.

[34] P. Navarro, *Souveraineté et surveillance, les enseignements tirés de l'affaire du Health Data Hub*, in *Revue Lamy droit de l'immatériel*, 2020/176.

[35] www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework.

[36] www.mediapart.fr/journal/france/221120/health-data-

later, and despite political reactions during the 2022 presidential elections,[37] the situation seems to be frozen. The problem is that very few cloud service-providers could meet the requirements of the Health Data Hub in terms of security and privacy from a technical point of view. There may not be many alternatives to undertake a project of this size with all the necessary privacy considerations and guarantees.[38]

The most relevant response should come from the European Union itself, in order to achieve a fully sovereign storage of these data. What remains is to develop a solution that can compete from a technical point of view with that of digital giants such as Microsoft. This is the ambitious objective of the European Health Data Space, a specific health ecosystem comprised of rules, common standards and practices, infrastructures and a governance framework.[39] The aim is to provide a trustworthy setting for secure access to and processing of a wide range of health data, including the opening of health data.

4. *Threats related to the opening of data and legal responses*

Health data are unique in that they need to be not only protected, but also opened, particularly for research purposes. In France, this principle of open access was established by the law of 26 January 2016[40] and reinforced by the law of 24 July 2019.[41] In European-Union law, this principle of open access is now also advocated by the Data Governance Act[42] (DGA), which allows protected data (for example data that is protected as personal data) to be made available.

However, one may wonder about the risks generated by such openness. Indeed, even if the regulation imposes security measures prior to the opening of these data, it has been shown that the risks of re-identification are exponential depending on the volume of data available. Latanya Sweeney's studies are particularly interesting on this subject, especially regarding health data.[43] The risk is that many data sets, when correlated, can allow re-identification of individuals. In the case of health data, the risks could be extremely high for the persons concerned. One solution to this problem would be to invest massively in the quality of anonymisation, which has a significant cost. However, the fees that the Regulation provides for public-sector bodies to authorise the re-use of such data are likely to be limited in practice.[44] Indeed, only the costs of processing requests will be taken into account in the calculation of the fee and not the real value of accessing and using such databases. Moreover, it is foreseeable that some States, such as France, will not charge for access to such data at all. Thus, notice n°6264/SG of 27 April 2021 on public policy on data, algorithms and source codes[45] states: "This renewed ambition implies, in addition, (...) the extinction, by 2023, of fees charged for the re-use of data, in particular on the basis of Article L. 324-1 of the Code of relations between the public and the administration". Although this notice predates the adoption of the regulation, it does not seem that the principle of free access therein advocated is likely to be called into question.[46]

This situation seems problematic, at a time when large sums of money must be invested to set up data warehouses and the European Health Data Space, as we have seen, but also and above all to carry out the crucial work of anonymising these data. Beyond the economic

hub-veran-s-engage-retirer-l-hebergement-microsoft-d-ici-deux-ans.

[37] www.lemonde.fr/pixels/article/2022/01/11/sante-coup-d-arret-pour-le-controverse-health-data-hub_6109065_4408996.html.

[38] P. Navarro, *Souveraineté et surveillance, les enseignements tirés de l'affaire du Health Data Hub.*

[39] www.health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

[40] Law of 26 January 2016 for the modernisation of French healthcare system.

[41] 24 July 2019 on the organisation and transformation of the healthcare system.

[42] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance).

[43] See for instance J. Su Yoo, A. Thaler, L. Sweeney and J. Zang, *Risks to Patient Privacy: A Re-identification of Patients in Maine and Vermont Statewide Hospital Data*, in www.techscience.org/a/2018100901.

[44] Art. 6 (5): "Fees shall be derived from the costs related to the processing of requests for re-use of the categories of data referred to in Article 3 (1). The methodology for calculating fees shall be published in advance".

[45] www.legifrance.gouv.fr/download/pdf/circ?id=

[46] In France, the report of the Bothorel Mission can be cited in the same vein: *Rapport Bothorel, Pour une politique publique de la donnée*, December 2020, 57. www.gouvernement.fr/rapport/11979-rapport-sur-la-politique-publique-de-la-donnee-des-algorithmes-et-des-codes-sources.

question[47] - should valuable data be made available to private companies for profit with taxpayers' money? - free access could well limit investments in the effective anonymisation of data and therefore in the legal security of their opening. This would seem to us highly questionable and provides an interesting opportunity to rethink our models of data opening and sharing. At a deeper level, a major challenge lies ahead: how can the European Union be both a model for personal-data protection and a champion of AI? Indeed, developing these AIs requires large amounts of learning data and can therefore generate legal risks. This is not an issue specific to health. Smart CCTV or predictive justice solutions raise for instance the same questions. But because of their sensitive nature, health data involve particular risks that must be taken into account.

In conclusion, the question of material, human and financial resources appears to be central: resources devoted to the technical and organisational security of information systems, to the sovereign storage of data, and to the safe opening of data. In a statement on 18 February 2021, President Macron stated: "Health structures will be invited to systematically devote 5 to 10% of their budget to cybersecurity, in particular to maintaining the security of information systems over time".[48] The political ambition on this point is therefore clear, but in the face of a public hospital in crisis, is cybersecurity really a priority? As for the European cloud, the example of Gaia-X[49] demonstrates the implementation difficulties encountered in the face of well-established giants such as Microsoft and AWS. In this context, it is easy to understand the fears inspired by the massive desire to open up data advocated by the DGA. Preserving our personal data has a price. Making the European Union an AI giant has a price too. The price of sovereignty.

[47] www.dsih.fr/article/4631/le-data-governance-act-ou-la-reutilisation-des-donnees-sans-veritable-valorisation.html.

[48] www.vie-publique.fr/discours/278659-emmanuel-macron-18022021-cybersecurite.

[49] www.lemondeinformatique.fr/actualites/lire-le-projet-europeen-gaia-x-est-bloque-au-stade-du-concept-86551.html.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 273-285
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 22

*Cybersecurity of Information Systems in the Public Healthcare Sector**

Carlos Galán Cordero
(Associate Professor of State Public Law and Administrative Law at Carlos III University of Madrid, Agencia de Tecnología Legal)

ABSTRACT In the digital era, where interconnection and immediacy in information management prevail, information systems have become essential assets for various institutions, and among them, the healthcare system stands out. In Spain, this system stores an enormous amount of sensitive data, ranging from clinical records to biomedical research, which are of interest not only to health professionals but also to malicious actors. Ensuring the cybersecurity of these systems is therefore not an option, but an absolute necessity. To face these challenges, the National Security Framework (ENS) in Spain establishes a series of measures, protocols and good practices aimed at protecting information and critical infrastructures, including healthcare infrastructures. This paper, although it also contemplates legislative actions emanating from the European Union, the United States and international initiatives, aims to analyse the importance of cybersecurity in the Spanish healthcare system, highlighting the relevance and applicability of the ENS in this context. We will address the main threats, current challenges and how the ENS guidelines provide a robust framework for effective defence.

1. *Introduction*

This paper, which is part of the research projects "Artificial intelligence in the national health system: solutions to specific legal problems" (PID2021-128621NB-I00) and "The impact of artificial intelligence on public services: A legal analysis of its scope and consequences in healthcare" (PGC2018-098243-B-I00) directed by Prof. Dr. José Vida Fernández and funded by the Spanish Ministry of Science and Innovation (MCIN/AEI/10. 13039/501100011033/) and by "FEDER: A way of doing Europe", aims to briefly present the regulatory framework for cybersecurity of public-information systems, especially when such systems are responsible for supporting public services in the field of healthcare.

2. *Information systems and cybersecurity*

2.1. *Information systems and cybersecurity concepts*

Before we dive into the subject and multifaceted content of cybersecurity, and in order to facilitate understanding, we should begin by recalling some essential concepts.

As with any scientific approach, the first thing to do is to define the field of our study: information systems and their cybersecurity.

Based on current regulations, we can define an information system as:[1]

Any of the following elements:

1. The electronic communications networks used by the entity within the scope of application of this royal decree over which it has management capacity.
2. Any device or group of interconnected or interrelated devices, in which one or more of them carry out, by means of a programme, the automatic processing of digital data.
3. Digital data stored, processed, retrieved or transmitted by means of the elements referred to in numbers 1 and 2 above, including those necessary for the operation, use, protection and maintenance of those elements.

In turn, we can define cybersecurity (or information systems security) as the ability of networks and information systems to withstand, at a given level of reliability, any action that compromises the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data, or the corresponding services offered by or accessible through such networks and information systems.[2]

It should be noted that, from these definitions, some conclusions can already be drawn:

* Article submitted to double-blind peer review.

[1] According to Annex IV-Glossary of Royal Decree 311/2022 of 3 May, regulating the National Security Framework (ENS)

[2] *Idem.* This definition also coincides with that contained in article 3 b) of Royal Decree-Law 12/2018, issued under the exclusive competences of the State in matters of telecommunications and general-communication regime (art. 149.1.21 CE) and public security (art. 149.1.29 CE), which defines the security of information networks and systems in the same way.

1. The concept of information system comprises any physical (*hardware*) or logical (*software*) element involved in the processing of data, whatever the data may be.
2. Cybersecurity does not seek to guarantee absolute immunity of the information systems concerned from threats at all times and in all situations - which is impossible to achieve - but rather to build a security model based on *resistance* measures - those that reasonably prevent the penetration of the attack and, in general, the progress of the cyber-incident - and on *resilience* measures - those aimed at recovering the full functionality of an information system once the cyber-incident is over.

2.2. *Cybersecurity as a manifestation of security*

Having defined the essential concepts of the work, we must go on to analyse to what extent *security* and *cybersecurity* are legally distinct concepts; an analysis that is not trivial, since, if they are located within a common protected legal asset, it could be deduced that the clarifications that could be made regarding either of them could be equally applicable.

First of all, we should mention the provisions of Law 36/2015, of 28 September, on National Security, which identifies cybersecurity in its article 10 as one of the "areas of special interest of national security... that require specific attention, as they are essential to preserve the rights and freedoms, as well as the well-being of citizens, and to guarantee the provision of essential services and resources".

Likewise, Law 8/2011, of 28 April, on measures for the Protection of Critical Infrastructures - defines them as strategic infrastructures "whose operation is essential and does not allow alternative solutions, so that their disruption or destruction would have a serious impact on essential services", issued under the competence attributed to the State by virtue of Article 149.1.29 of the Spanish Constitution (EC), it refers to cybersecurity. Article 2 of this Law defines strategic infrastructures as "the physical and information technology facilities, networks, systems and equipment on which the functioning of essential services is based", understanding that such services are those necessary for the maintenance of basic social functions, health, security, the social and economic well-being of citizens, or the efficient functioning of State institutions and public administrations.

Furthermore, the maintenance of cybersecurity is one of the functions of the National Intelligence Centre (CNI), as established in article 4 b) of Law 11/2002, of 6 May, regulating the National Intelligence Centre.

Finally, we should mention Royal Decree-Law 12/2018, of 7 September, on the security of networks and information systems, which transposes into Spanish law Directive (EU) 2016/1148 of the European Parliament and of the Council, of 6 July 2016, on measures to ensure a high common level of security of networks and information systems in the Union. The purpose of this regulation is to regulate the security of networks and information systems used for the provision of essential services and digital services and to establish an incident-notification system, as well as an institutional framework for its application and coordination between competent authorities and with the relevant cooperation bodies at EU level. As it is known, this Royal Decree-Law applies to essential services dependent on information networks and systems included in the strategic sectors defined in the annex to Law 8/2011, as well as to information-society services within the meaning of letter a) of the annex to Law 34/2002, of 11 July, on information-society services and electronic commerce.

The Constitutional Court has ruled on these issues in its judgment 142/2018 of 20 December 2018, in relation to the appeal of unconstitutionality 5284-2017 filed by the President of the Government regarding Law 15/2017, of 25 July, on the Cybersecurity Agency of Catalonia, on competences in the areas of telecommunications, defence and public security.[3]

By way of summary, the most significant consequences of the aforementioned judgement and the regulations it invokes are:

- Cybersecurity, as a synonym for network security, is an activity that is integrated into public security, as well as telecommunications. From its conceptualisation as a set of mechanisms aimed at protecting computer infrastructures and the digital information

[3] Boletín Oficial del Eestado, No. 22, Friday 25 January 2019.

they house, it is easy to infer that, as it is dedicated to the security of information technologies, it has a protective component that is specifically projected onto the specific area of the protection of networks and information systems used by citizens, companies and public administrations, (FJ 1).

- Cybersecurity is included in matters of state competence insofar as, by referring to the necessary actions of prevention, detection and response to cyberthreats, it affects issues related to public security and defence, infrastructures, networks and systems and the general telecommunications regime, (FJ 1).[4]

All these issues have been definitively consolidated in Royal Decree 1150/2021, of 28 December, approving the National Security Strategy 2021, in which public cybersecurity is configured as an integral part of National Security, cyberspace is included among the material objects of the security required of global common spaces, and the cybersecurity-governance model is integrated into the framework of the National Security System.

2.3. *The dimensions of cybersecurity*

As it has been pointed out,[5] cybersecurity is a multifaceted concept that can be studied from different points of view, taking into account precisely the guarantees required for the information processed or the services that must be preserved.

The National Security Framework (ENS), following the MAGERIT risk analysis and management methodology,[6] establishes five security dimensions: Confidentiality, Integrity, Authenticity, Traceability and Availability, to which we have added one more, of a generic nature: Legal Compliance.

The following table shows the definitions of these dimensions, as well as their applicability to the information processed or the services provided by the information systems concerned.

Cybersecurity dimension	Definition	Applicability
Confidentiality	The property or characteristic that information is neither made available nor disclosed to unauthorised individuals, entities or processes.	Information
Integrity	The property or characteristic that the information asset has not been altered in an unauthorised manner.	Information
Authenticity	The property or characteristic that an entity is who it claims to be or that it guarantees the source from which the data originates.	Information and Services
Traceability	The property or characteristic that the actions of an entity (person or process) can be indisputably traced back to that entity.	Information and Services
Availability	Property or characteristic of assets that authorised entities or processes have access to them when required.	Information and Services
Legal Compliance	Property or characteristic of the technologies, products, solutions or services that support operations, in order to remain permanently aligned with the provisions of applicable national, European or international legislation.	Information Systems, as a whole.

Of course, depending on the specific application or service in question, certain security dimensions will be more important

[4] Indeed, the aforementioned TC 142/2018 ruling states that "public security is, in principle, the exclusive competence of the State ex Article 149.1. 29 EC, a constitutional precept which shows that it already establishes exceptions ("without prejudice to") which, in a certain sense, come to modulate the exclusivity of State competence, proclaimed in the initial paragraph of Article 149 EC", adding that "*the exclusive competence of the State in matters of public security admits no exception other than that deriving from the creation of the autonomous police forces*" (STC 104/1989, of 8 June, FJ 3).

[5] Galán Pascual, Carlos Manuel. El Derecho a la Ciberseguridad, in Sociedad Digital y Derecho. Various authors. BOE, 2018.

[6] MAGERIT version 3: Information Systems Risk Analysis and Management Methodology. Available in: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

than others. In the case of telecommunications, all of them, to a greater or lesser extent, constitute the essential elements of cyber security, as will be seen throughout this chapter.

3. *The National Security Framework*

As we are dealing with information systems intended to provide public services, and therefore disregarding at this point the analysis of other regulations, we will focus on the assessment of the National Security Framework, implemented by Royal Decree 311/2022, of 3 May, which, among other areas of application that we will also comment on, regulates the (cyber)security of public-information systems.

Article 103.1 of the Spanish Constitution of 1978 proclaims: "The Public Administration serves the general interest objectively and acts in accordance with the principles of efficiency, hierarchy, decentralisation, deconcentration and coordination, with full submission to the Law".

Thus, generically protected by the inalienable principle of efficiency, the deployment of the services that the Public Sector (Public Administrations and the Institutional Public Sector) must provide to citizens, especially when using Information and Communication Technologies (ICT), requires - in order to comply with that constitutional requirement - the most appropriate administrative procedures, methods and tools to guarantee the security and reliability of their actions to all recipients: citizens and companies, but also the rest of the Public Sector.

Indeed, it would be of little use to have magnificent technologies that enable the processing and communication of millions of data if the actors involved in the life of administrative procedures did not perceive the information systems on which their relationship is based as secure infrastructures that are as reliable as the very essence that their activities require.

There is no doubt - as it has been stated - that better service to the citizen is the reason for the reforms that have been undertaken in Spain since the approval of the Constitution to configure a modern Administration that makes the principles of effectiveness and efficiency its ultimate reason, and always with an eye to the citizens and the general interest.

This interest was the main raison d'être of Law 11/2007, on Citizens' Electronic Access to Public Services (LAECSP, hereinafter), the original backbone of what has come to be known as e-Government, with the aim of keeping up with our times and the appropriate positioning of our Public Administrations in the European and international framework. The publication of Law 39/2015, of 1 October, on the Common Administrative Procedure of Public Administrations (LPACAP, hereinafter) and Law 40/2015, of 1 October, on the Legal Regime of the Public Sector (LRJSP, hereinafter), which repeal the previous one, consolidate the primacy of the use of electronic means in the development of public entities.

The general recognition of electronic relations in and with the public sector raises several questions that need to be considered:

- The increasing use of electronic means raises the question of the privacy of data provided electronically in connection with a file.
- Entitled parties have the right to access the status of the administrative procedure, as well as to examine the documents of which it is composed. This should at least be the case for a file initiated or processed electronically. Such a file should allow online access to parties interested in checking its status, without undermining privacy guarantees.
- In any case, the progressive use of electronic communications, derived from the recognition of the right to communicate electronically with the Administration, raises the question not only of how to adapt the Administration's human and material resources to a new way of relating with citizens, but also of how to adapt its actions and processing of files and, in general, rationalise, simplify and adapt procedures, taking advantage of the new reality imposed by ICTs.
- Recognising the right (obligation, in some cases) of citizens to communicate electronically with the Administration raises, firstly, the need to clearly define the electronic administrative headquarters with which relations are established, promoting a regime of identification, authentication, minimum content, legal protection, accessibility, availability and responsibility.

There are many precepts contained in our

administrative laws of reference (Law 39/2015 and Law 40/2015, both of 1 October) that insist on the need for the development of the Public-Sector entities.The development of procedures that respond to the general exercise of their competences must take place within the framework of an environment that contemplates all the security measures necessary to guarantee the integrity, confidentiality, authenticity and traceability of the information processed and the availability of the services provided, in compliance with the legislation in force.

Law 39/2015, of 1 October, includes, among the rights of individuals in their relations with Public Administrations, the one relating to "the protection of personal data, and in particular to the security and confidentiality of the data contained in the files, systems and applications of Public Administrations". It also makes various mentions of compliance with security guarantees and measures, when referring to registers, filing of documents and copies.

For its part, Law 40/2015, of 1 October, which includes the National Security Framework in Article 156, also mentions security when referring to administrations' electronic means of comunication and realtion, electronic headquarters, electronic filing of documents, electronic exchanges in closed-communication environments and data transmissions between Public Administrations.

The National Security Framework (ENS), currently operated by Royal Decree 311/2022 of 3 May, is one of the best European examples of cybersecurity treatment.

The current ENS, updated and heir to the one originally regulated in Royal Decree 3/2010 of 8 January, has the following objectives:

- To align the ENS to the existing regulatory framework and strategic context to ensure security in the digital administration, seeking to clearly reflect its scope of application for the benefit of cybersecurity and citizens' rights, as well as to update references to the current legal framework and review the formulation of certain issues in the light of this, in accordance with the National Cybersecurity Strategy 2019, so as to achieve simplification, precision or harmonisation of the mandates of the ENS, and to eliminate aspects that may have been considered excessive, or to add others identified as necessary.
- Introduce the ability to adjust the ENS requirements to ensure that they are adapted to the reality of certain groups or types of systems, taking into account the similarity of a multiplicity of entities or services in terms of the risks to which their information systems and services are exposed. This makes it advisable to include in the ENS the concept of a "Specific Compliance Profile" which, approved by the National Cryptologic Centre, allows for a more effective and efficient adaptation of the ENS, rationalising the resources required without undermining the pursued and enforceable protection.
- Facilitate a better response to cybersecurity trends, reduce vulnerabilities and promote continuous vigilance by revising basic principles, minimum requirements and security measures.

It should be remembered that the subjective scope of application of this regulation covers all entities included in the so-called Public Sector, in the terms defined in article 2 of Law 40/2015, of 1 October, and in accordance with the provisions of article 156. 2 of the same, being also applicable to the information systems of private-sector entities, when, in accordance with the applicable regulations and by virtue of a contractual relationship, they provide services or solutions to public-sector entities for the exercise of administrative powers and competences. This also applies, albeit in an instrumental manner, telecommunication operators and also extends to the supply chain of the aforementioned contractors or suppliers, to the extent necessary and in accordance with the results of the corresponding risk analysis.

In summary, the ENS consists of the basic principles and minimum requirements necessary for an adequate protection of the information processed and the services provided by the entities within its scope of application, in order to ensure access, confidentiality, integrity, traceability, authenticity, availability and preservation of the data, information and services used by electronic means that they manage in the exercise of their competences.

BASIC PRINCIPLES	MINIMUM REQUIREMENTS
- Security as an integral process. - Risk-based security	- Organisation and implementation of the security process.

management. - Prevention, detection, response and preservation. - Existence of lines of defence. - Continuous vigilance. - Periodic reassessment. - Differentiation of responsibilities.	- Risk analysis and management. - Personnel management. - Professionalism. - Authorisation and control of access. - Protection of installations. - Procurement of security products and contracting of security services. - Least privilege. - System integrity and updating. - Protection of information stored and in transit. - Prevention of other interconnected information systems. - Logging of activity and detection of malicious code. - Security incidents. - business continuity - Continuous improvement of the security process.

The ENS provides that entities within its scope of application adopt specific security measures, of organisational and technical nature, according to the following distribution:

Organizational framework	Security policy Security regulations Security procedures Authorization process
Operational framework	Planning (5 measures) Access control (6 measures) Operation (10 measures) External resources (4 measures) Cloud services Continuity of service (4 measures) System monitoring (3 measures)
Protective measures	Protection of facilities and infrastructure (7 measures) Staff management (4 measures) Protection of equipment (4 measures) Protection of communications (4 measures) Protection of information media (5 measures) Protection of IT applications (2 measures) Protection of information (6 measures) Protection of services (4 measures)

- Organisational framework: measures related to the overall security organisation.
- Operational framework: measures to protect the operation of the system as an integral set of components for a purpose.
- Protection measures: to protect specific assets, according to their nature, with the required level, in each security dimension.

As stated in the Royal Decree itself, the provisions of the ENS, insofar as they affect the information systems used for the provision of public services, must be considered to be included in the resources and procedures that the National Security System set out in Law 36/2015, of 28 September, on National Security.

The scope of application of the ENS is broad and logical, and extends to information systems:

- Of the entities of the entire public sector, as this term is defined in article 2 of Law 40/2015.
- That deal with classified information.
- Of private-sector entities when they provide services or solutions to the above, including the elements of the supply chain to the extent that a risk analysis so determines.

To ensure such compliance, the specifications for public tenders shall include the requirements in accordance with the ENS.

As telecommunications constitute an additional significant risk to ensure compliance with the aforementioned security dimensions, especially those of the latest generation, the reference to the installation, deployment and operation of 5G networks or the provision of 5G services by public-sector entities could not be left out of this new ENS.

Finally, the first additional provision of Organic Law 3/2018, of 5 December, on the Protection of Personal Data and guarantee of digital rights, confers on the ENS the inclusion of the measures that must be implemented in the event of processing of personal data to prevent their loss, alteration or unauthorised access, adapting the criteria for determining the risk in the processing of data to those established in article 32 of Regulation (EU) 2016/679, obliging the data controllers listed in article 77. 1 of this organic law to apply to the processing of

personal data the security measures that correspond to those provided for in the National Security Framework, as well as to promote a degree of implementation of equivalent measures in the companies or foundations linked to them even if subject to private law. An obligation that extends to cases in which a third party provides a service under a concession, management assignment or contract. In these cases, the security measures will correspond to those of the originating public administration and will be comply with the National Security Framework.

An interesting aspect of this new ENS are the so-called Specific Compliance Profiles, which comprise the set of security measures that, as a result of the mandatory risk analysis, are suitable for a specific security category, making it possible to adjust the ENS requirements to the specific needs of certain groups such as Local Entities, Universities, Paying Bodies, etc., or specific technological areas, such as cloud services, for example.

There is nothing to prevent the development of a specific Compliance Profile for information systems that provide public healthcare services, should the need arise.

Regarding the response to cyber incidents, the ENS states that public entities are obliged to notify the CCN-CERT of the security incidents of which they are victims, while private-sector organisations that provide services to public entities will notify INCIBE-CERT, which will immediately inform the CCN-CERT.

The CCN-CERT will technically determine the risk of reconnection of affected systems, indicating procedures to follow and safeguards to implement, and the General Secretariat for Digital Administration, of the State Secretariat for Digitalisation and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation, will authorise the reconnection to common means and services in its area of responsibility, if a CCN-CERT exposure surface report determines that the risk is assumable.

It should be noted that compliance with the ENS (and its public display) is achieved through two paths: a Self-Assessment, only applicable to information systems in the Basic security category; or a Formal Audit, applicable to information systems of any category (Basic, Medium or High), carried out by an ENS Certification Body previously accredited by the National Accreditation Body (ENAC), as provided for in the Resolution of 27 March 2018, of the State Secretariat for Public Administration, which approves the Technical Security Instruction on Information Systems Security Auditing and the Resolution of 13 October 2016, of the State Secretariat for Public Administrations, which approves the Technical Security Instruction in accordance with the National Security Framework.

Finally, the ENS confers the General Secretariat for Digital Administration (of the Secretariat of State for Digitalisation and Artificial Intelligence of the Ministry of Economic Affairs and Digital Transformation) and the National Cryptologic Centre (attached to the National Intelligence Centre of the Ministry of Defence), within their respective competences, the responsibility to ensure the proper implementation, development and monitoring of the ENS in the entities within its scope of application.

4. *The most significant European and international regulations on the matter*

In relation to the regulation of the cybersecurity of medical devices, the European Union has taken two particularly significant approaches:

- Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC (hereinafter MDR Regulation).
- Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in-vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU (hereinafter IVDR Regulation).

Both regulations focus on ensuring that devices placed on the EU market are prepared to deal adequately with cyber threats by establishing certain essential cybersecurity requirements, requiring manufacturers of such devices to take appropriate measures during their manufacture taking into account these risks, based on the security dimensions mentioned above, in particular the confidentiality and integrity of the information processed by such devices, ensuring their

availability and controlling access to them.

Cybersecurity is explicitly addressed in Annex I, sections 17.2, 17.3, 17.4 and 18.8 of the MDR, namely:

> 17.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
> 17.3. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).
> 17.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.
> …
> 18.8. Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended.

Cybersecurity is similarly addressed in Annex I, sections 16.2, 16.3 and 16.4 of the IVDR Regulation, namely:

> 16.2. For devices that incorporate software or for software that are devices in themselves, the software shall be developed and manufactured in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation.
> 16.3. Software referred to in this Section that is intended to be used in combination with mobile computing platforms shall be designed and manufactured taking into account the specific features of the mobile platform (e.g. size and contrast ratio of the screen) and the external factors related to their use (varying environment as regards level of light or noise).
> 16.4. Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

On the other hand, and as the healthcare sector is one of the most important areas for guaranteeing the maintenance of the cybersecurity of the information systems used for healthcare, the Directives colloquially known as the NIS Directive and the NIS Directive2 should be added to the list of important regulations.

Indeed, what has come to be known as the NIS Directive (Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to ensure a high common level of security of network and information systems in the Union), published in the OJEU on 19 July 2016, considered it essential for all EU Member States to have minimum capabilities and a strategy to ensure a high level of security of network and information systems on their territory, especially with regard to what the European standard defined as operators of essential services and digital-service providers, which should result in the adoption of a set of cybersecurity measures aimed at improving the functioning of the internal market.

The ultimate addressees of the regulation are shown in the table below:

Operators of essential services, in the sectors…[7]
Energy: electricity, oil and gas.
Transport: air, rail, maritime and inland waterway and road.
Banking.
Financial market infrastructures.
Health sector: health care environments (including hospitals and private clinics).
Drinking-water supply and distribution.
Digital infrastructure: IXP, DNS Service Providers and Top Level Domain Name Registries.
Digital service providers
Online marketplaces.
Online search engines.
Cloud computing services.

The criteria for the identification of essential operators were:

[7] Provided that they are: a) an entity providing a service essential to the maintenance of crucial social or economic activities; b) the provision of that service depends on networks and information systems; and c) an incident would have significant disruptive effects on the provision of that service.

a) It provides a service essential for the maintenance of crucial social or economic activities;
b) The provision of such a service is dependent on networks and information systems; and
c) An incident would have a significant disruptive effect on the provision of that service.

The NIS Directive, in summary

a) Established an obligation for all Member States to adopt a national strategy for the security of network and information systems;
b) Established a Cooperation Group to support and facilitate strategic cooperation and information exchange between Member States and to develop trust and confidence between them;
c) Established a network of Computer Security Incident Response Teams (CSIRT Network[8]), in order to contribute to the development of trust and security between Member States and to promote rapid and effective operational cooperation;
d) Established security and notification requirements for operators of essential services and for digital-service providers;
e) Established obligations for Member States to designate competent national authorities, single points of contact and CSIRTs with functions related to the security of network and information systems.

On 8 September 2018, the Official State Gazette published Royal Decree-Law 12/2018, of 7 September, on the security of networks and information systems, fulfilling the mandate to transpose the NIS Directive.

Although the Directive from which it stemmed limited its scope of application to the so-called "operators of essential services" and "digital-service providers", the Spanish law took advantage of the mandate to extend its scope to sectors not expressly included in the European Directive (without this entailing a covert repeal or regulatory displacement of the Spanish legislation in force). Significant examples of this extension are trust-service providers or operators of electronic-communication networks and services, which are included among those covered by the regulation, insofar as they may be designated as critical operators.

At this point, it is worth noting the effort made by the working group drafting the RD-Law to harmonise the three state regulations of special significance in the area of (cyber)security: Royal Decree 3/2010, of 8 January, which regulates the National Security Framework (ENS),[9] Law 8/2011, of 28 April, which establishes measures for the protection of Critical Infrastructures, and Law 36/2015, of 28 September, on National Security.[10]

The governance model set out in this RD-Law is based on the scheme of competences that the current National Security and Cybersecurity Strategies have drawn up: the National Security Council, the National Cybersecurity Council, the Competent Authorities and the reference CSIRTs, conferring on the so-called Competent Authorities the functions of supervision, surveillance and sanctioning, reserving for the reference CSIRTs the more operational functions, such as risk analysis and national-operational management of the response to incidents, a national action protected by the provisions of art. 1491.29 of our Constitution, which confers exclusive powers on the State in matters of national security, cybersecurity being one of its manifestations, as we have pointed out above.

These reference CSIRTs constitute, in our opinion, the cornerstone on which the treatment of cybersecurity rests, since, beyond the functions legally granted to the Competent Authorities, they materialise the mechanisms for prevention, detection and response to incidents. As of the entry into force of this new RD-Law, these functions require maximum coordination from all of them, as also provided for in the regulation, which confers on the CCN-CERT (of the National Cryptologic Centre, attached to the National Intelligence Centre) the function of national coordinator in cases of particular seriousness.

Despite being a regulation in force and therefore enforceable, the Royal Decree-Law postponed certain issues to its regulatory development, which we will see below.

At present, there are numerous regulations with a technological substratum that prescribe the notification of incidents to the competent

[8] *Computer Security Incident Response Team.*

[9] Recently repealed by Royal Decree 311/2022 of 3 May, which regulates the National Security Framework.

[10] We recall that the strategic sectors defined in Law 8/2011, of 28 April, are: Administration; Space; Nuclear Industry; Chemical Industry; Research Facilities; Water; Energy; Health; ICT; Transport; Food and the Financial and Tax System.

body. This diversity, which often applies to the same obliged subject, encourages and justifies the existence of a Common Platform for incident notification, capable of providing a response, through a single process (including initial, intermediate and final notification) automatically addressed to each competent authority by virtue of the legislation affected, which may constitute, in our opinion, one of the most innovative measures of this Royal Decree-Law in cybersecurity matters, in the image of what the CCN-CERT has been developing in the Public Sector with the LUCIA platform.

The RD-Law exhibits a particularly-rigorous infringement regime. Just one example: in certain circumstances, it classifies as very serious the failure to adopt measures to remedy the deficiencies detected or repeated failure to comply with the obligation to notify incidents.

The regulatory development referred-to above took place by Royal Decree 43/2021 of 26 January, which regulated the following aspects:

- The identification of specific factors in the sectors of essential service operators to determine whether an incident could have significant disruptive effects.
- In the determination of the Competent Authorities, the corresponding sectoral authority by reason of the subject matter, when critical operators are not involved.
- Within the functions of the Competent Authorities, the establishment of communication channels with the operators of essential services and digital-service providers, and the protocols for coordination with the reference CSIRTs.
- The identification of essential service operators with an impact on National Defence.
- The determination of particularly serious cases that require the national coordination of the CCN-CERT.
- Determination of the coordination mechanisms of the reference CSIRTs with the Cybernetic Coordination Office of the National Centre for Infrastructure Protection and Cybersecurity of the Ministry of the Interior, when the response activities may affect a critical operator.
- Determining the technical and organisational measures to be adopted by operators of essential-service and digital-service providers.
- The setting of deadlines for the designation and communication to the Competent Authority by the operators of essential services of the person, unit or collegiate body responsible for information security and the identification of their functions.
- Identification, for notification purposes, of events or incidents that could affect networks and information systems, even if they have not yet done so.
- The identification of the necessary measures concerning the notification of incidents by operators of essential services.
- The body of the authority competent to impose penalties in the case of serious or minor infringements.

A new Directive, colloquially referred to as NIS2, was published at the end of 2022, repealing the previous one, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2016/1148.

Indeed, during the second half of 2020, the European Commission carried out an evaluation of the results achieved with the NIS Directive, including a public consultation that concluded, from various perspectives, the need to improve the transposition of the standard, its scope and its definition.

As a result, the Commission presented a proposal for a revision[11] that sought to improve some of the problems that the first NIS Directive had not solved and which, as mentioned,[12] appeared in the above-mentioned evaluation, such as low business cyberresilience, different implementation from country to country, low situational awareness and lack of common responses.

In its Explanatory Memorandum, the Commission acknowledges that:

- 'The scope of the NIS Directive has become too small due to the advance of digitisation and connectivity in recent years and does not include relevant digital services.

[11] Commission Proposal for a Directive COM (2020) 823 (final) of 16 December on measures for a high common level of cybersecurity in the EU and Annexes on critical and important entities.

[12] F. Arteaga, *La evaluación y la revisión de la Directiva NIS: la directiva NIS2.0*, in *R.I. Elcano*, Feb. 2021

- It also does not include all relevant actors because the criteria in the Directive and in the national transpositions for identifying digital service providers have not been clear.
- For the same reasons, the procedure for incident reporting by providers of essential services is not the same and the sanctions and enforcement obligations vary in each Member State.
- The exchange of information between public and private actors remains very low and unsystematic.
- The disparity in the budgetary and human resources available to the Member States affects their level of maturity and their cyber-resilience capacity.

The new Directive thus reflects the Commission's desire to extend the scope of application of the European standard to other actors, such as providers of public communication services or networks, content or data providers, social-networking platforms and those dedicated to fostering trust in the above or to public administrations, postal services, water management, space, food, among others, eliminating the current classification of operators of essential services and digital-service providers, replacing them with essential entities and important entities.

The classification by sector of the entities covered by the new NIS2 Directive is as follows:

Essential Entities	Important Entities
- Energy (Electricity, District Heating and Cooling, Oil, Gas, Hydrogen) - Transport (Air, Rail, Water, Road). - Banking. - Financial market infrastructures. - Health. - Drinking water. - Wastewater. - Digital infrastructure.[13]	- Postal and courier services. - Waste management. - Chemical manufacturing, production and distribution. - Food production, processing and distribution. - Manufacturing.[14] - Digital providers (Online marketplaces, Online search engines, Social networking service platforms). - Research.
- Public administrations - Space.	

In both groups, the new text obliges states to supervise (by means of *ex ante* or *ex post* actions, depending on their affiliation) the security measures to be adopted by the entities affected, which, in the event of non-compliance, would entail significant sanctions.

Once again, prior risk analysis, as a method for determining the appropriate security measures, is also an essential element of this new regulation, as it has already been, for example, in the Spanish case with the National Security Framework analysed above.

Finally, in response to calls for action by the Council[15] and the Parliament[16] to review the current approach to the security of critical entities and ensure greater harmonisation with the NIS Directive, Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC aims to improve the provision in the internal market of services that are essential for the maintenance of vital societal functions or economic activities, by enhancing the resilience of critical entities providing such services, addressing the increased interconnection between the physical and digital world through a legislative framework with robust resilience measures for both cyber and physical aspects, as set out in the Strategy for a Security Union.[17]

As its introductory text points out, the

[13] These include: - Internet Exchange Point providers - DNS service providers, excluding root name server operators - TLD name registries - Cloud computing service providers - Data centre service providers - Content delivery network providers - Trusted service providers referred to in point (19) of Article 3 of Regulation (EU) no. No 910/2014(1) - Providers of public electronic communications networks as referred to in point (8) of Article 2 of Directive (EU) 2018/1972(2) or providers of electronic communications services as referred to in point (4) of Article 2 of Directive (EU) 2018/1972 where their services are publicly available. ICT Service Management (B2B); ICT Service Management (B2B); Managed Service Providers (MSP) - Managed Security Service Providers (MSSP).

[14] Manufacture of medical devices and in-vitro diagnostic medical devices; computer, electronic and optical products; machinery and equipment n.e.c.; motor vehicles, trailers and semi-trailers and other transport equipment.

[15] Council conclusions of 10 December 2019 on complementary actions to increase resilience and combat hybrid threats (doc. 14972/19).

[16] Report on the conclusions and recommendations of the European Parliament's Special Committee on Terrorism (2018/2044 (INI)).

[17] COM(2020) 605.

standard reflects national approaches that emphasise cross-sectoral and cross-border interdependencies, where protection is only one element alongside risk prevention and mitigation, business continuity and recovery (resilience).

This Directive therefore aims to:

- Establish obligations on Member States to take certain measures aimed at ensuring the provision in the internal market of services essential for the maintenance of vital societal functions or economic activities, in particular to identify entities and critical entities to be considered as equivalent in certain respects and to enable them to fulfil their obligations;
- Establish obligations on critical entities aimed at increasing their resilience and improving their ability to provide such services in the internal market;
- To lay down rules on the supervision and enforcement of critical institutions, and the specific supervision of critical institutions considered to be of particular European importance.

The scope of application covers (public or private) entities falling in the types mentioned in its Annex, and identified as "critical entities" by a Member State. In accordance with Article 5 of the Directive, the types of entities related to the Digital Infrastructure sector are the following:

- Internet Exchange Point Providers (from the NIS2 Directive).
- DNS service providers (from the NIS2 Directive).
- Top Level Domain Name Registries (from the NIS2 Directive).
- Cloud computing service providers (from the NIS2 Directive).
- Data centre service providers (from the NIS2 Directive).
- Content delivery network providers (from the NIS2 Directive).
- Providers of trust services referred to in Article 3(19) of Regulation (EU) No 910/2014 (eIDAS Regulation).
- Providers of public electronic communications networks as referred to in Article 2(8) of the already discussed Directive 2018/1972/EU (European Electronic Communications Code) or providers of electronic communications services within the meaning of Article 2(4) of Directive (EU) 2018/1972, to the extent that their services are available to the public.

This also includes providers of public electronic-communication networks.

We cannot conclude this review of European initiatives on the subject without mentioning the work being carried out by ENISA (European Union Agency for Cybersecurity), in particular its research and dissemination work.

In this regard, and in the aspects that interest us now, we should highlight the document *Cybersecurity and Privacy in AI - Medical Imaging Diagnosis* (June 2023), an in-depth study, that for the first time identifies the assets, the actors, their roles, the relevant processes, the AI algorithms used and the cybersecurity and privacy requirements.

Drawing on previous ENISA work, such as the *Securing Machine Learning Algorithms* report, as well as legislation such as the GDPR, the paper has identified the cybersecurity and privacy threats and vulnerabilities that can be exploited in the scenario under consideration. While the focus is on threats and vulnerabilities related to *Machine Learning* techniques, broader AI-related considerations have also been taken into account.

It is worthwhile to spend a few lines examining the state of play of this issue in the United States.

A number of authors[18] have been urging the U.S. Food and Drug Administration (FDA) to take action on this issue and develop a new regulatory framework to address the risks of cyber threats to medical devices, arguing that cyber-physical medical devices pose new challenges to the FDA's traditional approach to assessing their safety and effectiveness because, unlike other software, cyber-physical devices are embedded in an unpredictable and limitless environment and that, unlike traditional-hardware devices, risks to patients can arise not only from malfunction but also from malicious external agents.

Although there is no clear FDA guidance on this issue, the FDA has been issuing a series of guidance focused on cybersecurity, most recently in 2023.[19] These guidance

[18] Such as Christopher S. Yoo and Bethany Lee of the University of Pennsylvania Carey Law School in their paper *Optimising Cybersecurity Risk in Medical Cyber-Physical Devices*.

[19] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions -

documents recognise that residual risks are unavoidable and that certain risk-acceptance criteria must be established for medical devices to be considered "trustworthy".

Finally, at the global level, it is important to mention the *Medical Device Cybersecurity Guide*[20] by the Medical Device Regulators Forum (IMDRF), which aims to promote a globally-harmonised approach to medical-device cybersecurity.

This Forum has published the following papers:

- Technical document (IMDRF/CYBER WG/N73) Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity (13 April 2023).[21]
- Technical document (IMDRF/CYBER WG/N70) Principles and Practices for the Cybersecurity of Legacy Medical Devices (11 April 2023).[22]
- Technical document (IMDRF/CYBER WG/N60) Principles and Practices for Medical Device Cybersecurity (20 April 2020).[23]

These IMDRF technical documents provide guidance including, among other issues, definitions of medical-device cybersecurity, shared responsibility of stakeholders and information sharing.

5. *Conclusions*

As we have been able to analyse in the preceding paragraphs, as far as Spain is concerned and in view of the risks derived from operating in cyberspace, cybersecurity is a *sine qua non* condition for the adequate provision of public services, without which the principles of public attention set out in our administrative laws, in the National Security Strategy and in the Constitution cannot be met.

Therefore, having discarded from its scope of application the current wording of the Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020 medical devices for human use (regulated in Regulation (EU) 2017/745), the cybersecurity model to be applied to information systems (and their individual constituent elements) aimed at providing healthcare services must comply with the provisions of the aforementioned Royal Decree 311/2022, of 3 May, regulating the National Security Framework, which we have reported on in these pages.

Now is the time, therefore, to generate confidence in the ultimate recipients of healthcare services, guaranteeing that the information systems used by public entities in their provision are secure and reliable.

Guidance for Industry and Food and Drug Administration Staff. (27 September 2023).

[20] Medical Device Cybersecurity Guide; see: http://www.imdrf.org/workitems/wi-mdc-guide.asp

[21] https://www.imdrf.org/documents/principles-and-practices-software-bill-materials-medical-device-cybersecurity

[22] https://www.imdrf.org/documents/principles-and-practices-cybersecurity-legacy-medical-devices

[23] https://www.imdrf.org/documents/principles-and-practices-medical-device-cybersecurity

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 287-297
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 23

*Health and Cybercrime**

Francesco Saverio Romolo
(Associate Tenured Professor of Legal Medicine at University of Bergamo)

Simone Grassi
(Type B University Researcher in Legal Medicine at University of Florence)

Alessandro Di Luca
(Medical Legal Expert at Coordinamento Generale Medico Legale of INPS)

Michela Previtali
(Degree in Law at University of Bergamo)

Antonio Oliva
(Full Professor of Legal Medicine at Università Cattolica del Sacro Cuore-Fondazione Policlinico Universitario A. Gemelli IRCCS, Rome)

ABSTRACT The importance of confidentiality in the practice of medical profession was recognised as a priority since the Hippocratic Oath. Internet caused a revolution not only in everyday life of citizens but also in the handling of health information by medical professionals. Exchange of health data can guarantee a better answer to the population health needs but also poses new risks. The European Union Agency for Network and Information Security (ENISA) published its first analysis of the cyber threat landscape of the health sector in the EU in July 2023.
Hospitals faced many different cyberattacks in the last years, sometimes with important economic consequences. This article reports the main classes of possible attacks, such as phishing, ransomware, data loss or data theft, attacks to connected medical devices, and Distributed-Denial-of-Service (DDoS), and the specific targets attractive for cybercriminals in the health information technologies (HIT), such as the electronic health records (EHR), the personal health records (PHR), the booking system for clinical appointments and the administrative systems. From a medico-legal perspective, it is paramount to frame in a correct manner the issue regarding current cybercrimes targeting healthcare structures.
The issue is well known for Patient Safety operators as a serious threat: a delay on data availability or the impossibility to obtain certain information in critical occasion could led to serious (if not fatal) consequences for the patient.
After examining the laws involved in protecting patients and their data from cyberattwacks, we conclude that addressing these threats cannot be solely based on legal means, but also IT and risk management strategies, together with the compliance with standards such as ISO 31000 are needed for a fruitful approach with a specific focus on digital expertise of healthcare professionals as well as administrative staff involved in healthcare.

1. *Health data*

1.1. *Historical introduction: from the Hippocratic Oath to the European Charter of Medical Ethics*

Confidentiality in the practice of medical profession is recognised as a priority since the time when the Hippocratic Oath was written.[1] The Hippocratic Oath demands physician to respect confidentiality: "What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about".[2]

In 1949 the World Medical Association published the first International Code of Medical Ethics (ICoME).[3]

The comparative studies of health legislation in Europe[4] prepared ground for the WHO Declaration on the Promotion of Patients' Rights in Europe, drafted in 1994, including the definition of the concept of medical secrecy: "4.1 All information about

* Article submitted to double-blind peer review.

[1] D.C. Smith, *The Hippocratic Oath and Modern Medicine*, in *Journal of the History of Medicine and Allied Sciences*, vol. 51, issue 4, 1996, 484–500.

[2] S.A. Antoniou, G.A. Antoniou, F.A. Granderath *et al.*, *Reflections of the Hippocratic Oath in Modern Medicine*, in *World J. Surg*., vol. 34, 2010, 3075–3079.

[3] World Medical Association published, *International Code of Medical Ethics*, available online at www.wma.net/policies-post/wma-international-code-of-medical-ethics.

[4] J.J. Leenen, G. Pinet and A.V. Prims, *Trends in health legislation in Europe*, WHO 1986.

patient's health status, medical condition, diagnosis, prognosis and treatment and all other information of a personal kind must be kept confidential, even after death. 4.2 Confidential information can only be disclosed if the patient gives explicit consent or if the law expressly provides for this. Consent may be presumed where disclosure is to other health care providers involved in the patient's treatment. 4.3 All identifiable patient data must be protected. The protection of data must be appropriate to the manner of their storage. Human substances from which identifiable data can be derived must be likewise protected".[5]

Internet caused a revolution in everyday life including the handling of health data. Their exchange among healthcare professional can guarantee a better answer to the requests of health from patients but also poses new risks of mishandling of information related to the health condition of people.

On 10 June 2011 the European Charter of Medical Ethics was adopted.[6] According to its Principle 5 "The physician is the patient's essential confidant. He betrays this confidence on revealing what he has learned from the patient". Based on this principle, Deontological Guidelines were established by the European Council of Medical Orders (ECMO), stating about professional secrecy: "The physician must ensure the patient absolute secrecy on all the information he has collected. Confidentiality covers everything that physicians have learned in the exercise of their profession, that is to say not only what they were told in trust, but also what they may have observed, heard or understood. Medical confidentiality is not abolished by the death of patients. The physician informs people assisting him about their obligations as regards secrecy, asking, whenever possible to give a written undertaking. Derogations, when they exist, are strictly provided for in national legislations".

The importance of the subject pushed the establishment of the Task Force on Privacy and the Protection of Health-Related Data in 2017 by the UN Special Rapporteur on the right to privacy. Its aim was to prepare a recommendation on the protection and use of health-related data for Member States to use as an international baseline of minimum data protection standards for health-related data.[7]

1.2. *Personal data in Europe*

The article 8 of the Charter of fundamental rights of the European Union is about the "Protection of personal data" and states that: "1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".[8]

The need to reduce or avoiding the risks connected to wrongful processing of data resulted in the Data Protection Directive in 1995.[9] On 25 January 2012 the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules[10] and in 2016 the EU adopted the General Data Protection Regulation (GDPR), applicable as of 25 May 2018 in all member states.[11]

According to GDPR, anyone who decides 'why' and 'how' personal data are processed is a data controller. Among the tasks the data controller must fulfil is the implementation of appropriate technical and organisational

[5] M.E. Sokalska, *Medical Confidentiality – Quo Vadis?*, in *European Journal of Health Law*, vol. 11, issue 1, 2004, 35-43.

[6] *European Charter of Medical Ethics*, 2011, available online at www.ceom-ecmo.eu/sites/default/files/documents/en-european_medical_ethics_charter-adopted_in_kos.pdf.

[7] UN Special Rapporteur on the right to privacy, *Report on the Protection and Use of Health-Related Data*, 2019.

[8] European Union: Council of the European Union, *Charter of Fundamental Rights of the European Union* (2007/C 303/01), 14 December 2007, C 303/1, available at: www.europarl.europa.eu/charter/pdf/text_en.pdf.

[9] European Union. Directive (EC) 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 ('Directive 95/46/EC').

[10] V. Reding, *The European data protection framework for the twenty-first century*, in *International Data Privacy Law*, vol. 2, No. 3, 2012, 119-129.

[11] European Union, Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), which was approved and come into force on 27 April 2016, (2016) available at https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679 last access on 12 July 2023.

protection measures against data breach. A 'personal data breach' is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. A possible approach to protect personal data is to render them unintelligible to any person who is not authorised to access it (encryption).

In recent years, physicians and patients have been extensively using computerized technologies and digital information. Data related to health are collected by physicians and shared through network systems. The central ethical issue stemming from the use of electronic records is the need for an equilibrium between the right to health and the risk of leaking confidential medical information.

The GDPR defines 'data concerning health' as personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status. This definition is an extensive one because it regards even the data that can reveal the health status or risk of patient only if combined with other information[12]. Health data can be processed if the patient, called "data subject", has given consent to their processing for one or more specific purposes.

The main reason to collect health data is to support the delivery of healthcare (this use is known as the "primary use of data").[13] The recent COVID-19 outbreak clearly demonstrated how access to health data is also important for scientific research and policy-making purposes (known as the "secondary use of data").[14] [15] According to GDPR, the explicit consent of the data subject can be waived, for example, for reasons of substantial public interest or for scientific research.[16]

The EU Commission published in May 2022 a proposal for a regulation of the European Parliament and of the Council on the European Health Data Space (EHDS), seeking to ensure the people's control over their health data, allow harmonised and interoperable electronic health record (EHR) systems across the EU and build a framework for the secondary use of health data for research, innovation and policymaking to improve population's health.[17]

The right to the protection of health data is not an absolute right anymore, protected by professional secrecy; it must be considered nowadays "in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality".[18]

The massive quantities of health data collected over the last decades resulted in growing enthusiasm for the potential usefulness of these in transforming personal care, clinical care and public health.[19]

The use of Big Data in healthcare poses not only new ethical and legal challenges because of the personal nature of the information involved but also new technical and organisational challenges related to the need of allowing effective exchange and use of health data while protecting them by attacks aiming to possible illegal use (e.g. data breaches).[20]

2. *Cybercrime targeting the healthcare system*

According to EU Cybersecurity Act, a cyber threat is "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such

[12] V. Hordern, *Data protection compliance in the age of digital health*, in *Eur. J. Health Law*, vol. 23, 2016, 248-264.
[13] R. Hussein, L. Scherdel, F. Nicolet and F. Martin-Sanchez, *Towards the European Health Data Space (EHDS) ecosystem: A survey research on future health data scenarios*, in *Journal of Medical Informatics*, vol. 170, 2023, 104949.
[14] C.J. Wang and R.H. Brook, *Response to COVID-19 in Taiwan: big data analytics, new technology, and proactive testing*, in *JAMA*, vol. 323, 2020, 1341-1342.
[15] C. Cosgriff, D. Ebner and L. Celi, *Data sharing in the era of COVID-19,* in *Lancet Digit Health*, 2020, no. 2224.
[16] A. Oliva, S. Grassi, G. Vetrugno, R. Rossi, G. Della Morte, V. Pinchi and M. Caputo, *Management of Medico-Legal Risks,* in *Digital Health Era: A Scoping Review*, in *Front. Med*., vol. 8, 2022, 821756.
[17] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, available online at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0197, 2022.
[18] European Union, General data protection regulation, Off J Eur Union 49 (2016) L119 available online at https://gdpr-info.eu.
[19] E. Vayena, J. Dzenowagis, J.S. Brownstein and A. Sheikh, *Policy implications of big data in the health sector*, in *Bull World Health Organ*, 2018, no. 96, 66–8.
[20] R. Pastorino, C. De Vito, G. Migliara, K. Glocker, I. Binenbaum, W. Ricciardi and S. Boccia, *Benefits and challenges of Big Data in healthcare: an overview of the European initiatives*, in *European Journal of Public Health*, vol. 29, 2019, issue supplement 3, 23–27.

systems and other persons".[21] The Cybersecurity Act followed the Directive 2016/11481 on security of network and information systems (the NIS Directive), which was the first EU legislation for the protection of network and information systems across the Union.[22] The trust in digital technologies is especially needed in many sectors which are vital for the society, including healthcare, which are suffering deliberate attacks to their network and information systems by criminals in recent times. Any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT) can be defined as cyber-dependent crime. An example is the creation and spread of malware, but criminals also hack to steal sensitive personal or industry data or attacks to cause denial of service, resulting in financial and/or reputational damage.[23]

Malwares are the most frequent sort of computer, network, or user attacks to cause damage or steal sensitive information.[24] Healthcare facilities must now deal not only with malwares but with many different cyber risks, i.e. "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems".[25]

The European Union Agency for Network and Information Security (ENISA) was founded in 2004 as the specialised EU agency. ENISA published its first analysis of the cyber threat landscape of the health sector in the EU, reporting cyber incidents from January 2021 to March 2023 in the health sector in July 2023.[26]

2.1. *A little history about health and cybercrime*

It is interesting that the first ransomware attack had a healthcare theme. In 1989 Joseph Popp, an AIDS researcher, distributed thousands of 'floppy disks' to other AIDS researchers, spreading a malware across more than 90 countries. The software locked the computer and showed on the screen the request for a payment when the system was powered on 90 times.[27]

In the following years hospitals were attacked in many different ways, sometimes with important economic consequences. An example occurred on 20 March 2014, when numerous hosts attacked the Boston Children's Hospital, causing a network outage called Distributed Denial of Service (DDoS), adversely disrupting hospital operations for two weeks.[28]

In April 2014 attackers gained access to the database of Anthem, the second largest health insurance company in the USA.[29] The breach originated from an employee, who opened a phishing email, allowing the threat actor to gain access to the employee's computer. The attack was first discovered on 27 January 2015 and affected not-encrypted personally identifiable information (PII) of almost 80 million customers, including records of at least 12 million minors, and alerted federal authorities.[30] In August 2018 the final

[21] European Union, Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), available online at https://eur-lex.europa.eu/eli/reg/2019/881/oj.

[22] D. Markopoulou, V. Papakonstantinou and P. de Hert, *The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation*, in *Computer Law & Security Review*, vol. 35, 2019, issue 6, 105336.

[23] Europol, *Internet Organised Crime Threat Assessment 2018* (2019), available online at www.europol.europa.eu/internet-organised-crime-threat-assessment-2018.

[24] F.A. Aboaoja, A. Zainal, F.A. Ghaleb, B.A.S. Al-rimy, T.A.E. Eisa and A.A.H. Elnour, *Malware Detection Issues, Challenges, and Future Directions: A Survey*, in *Applied Sciences*, 12, 2022, 1.

[25] A. Sardi, A. Rizzi, E. Sorano and A. Guerrieri, *Cyber Risk in Health Facilities: A Systematic Literature Review*, in *Sustainability*, vol. 12, 2020, 1. doi: https://doi.org/10.3390/su12177002.

[26] European Union Agency for Network and Information Security, *ENISA Threat Landscape: Health Sector*, available online at www.enisa.europa.eu/publications/health-threat-landscape.

[27] C. Mehra, AK. Sharma and A. Sharma, *Elucidating Ransomware Attacks in Cyber-Security*, in *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, vol. 9, Issue 1, 2019, 3536-3541.

[28] *Cybersecurity in Healthcare: A Review of Recent Attacks and Mitigation Strategies*, available online at www.proquest.com/openview/c5af58f60f7c269ac04918fa2382f05e/1?pqorigsite=gscholar&cbl=544481.

[29] Y.Y. Leong and Y.C. Chen, *Cyber risk cost and management in IoT devices-linked health insurance*, in *Geneva Pap Risk Insur Issues Pract 45*, 2020, 737–759.

[30] L.H. Yeo and J. Banfield, *Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis*, in *Perspect. Health Inf Manag*, 2022 Mar 15; 19 (Spring) available online at www.ncbi.nlm.nih.gov/pmc/articles/PMC9123525/#B2

approval was given to a $115 million settlement that ended further claims against Anthem over its data breach.[31] In October 2020 a coalition made up of 44 states and Washington D.C. reached a $39.5 million settlement with Anthem, to resolve the claims stemming from the 2014 cyberattack.[32]

Another example is what happened on February 2016, when Hollywood Presbyterian Medical Center was attacked by a ransomware, disrupting the systems and making patient data unusable. It was the first attack that put human lives at risk (threatening to turn off life-saving equipment) and the Medical Center paid the 40 bitcoins ransom ($17,000 in 2016) to recover their files.[33]

A global ransomware attack, called WannaCry, struck about 200,000 systems across 150 countries on 12 May 2017. Only considering the British National Health Service (NHS), at least 80 out of 236 trusts across England were affected: 34 infected hospital trusts (NHS organisations that provide acute care, specialised medical services, mental healthcare, or ambulance services) were locked out of their digital systems and medical devices, such as Magnetic resonance imaging (MRI) scanners; 46 affected hospital trusts were not infected but reported disruption. Appointments cancelled identified by NHS England were 6,912, but calculations based on the normal rate of follow-up appointments to first appointments estimated more than 19,000 appointments cancelled.[34] Hospitals directly infected with the ransomware had 4% fewer emergency admissions and 9% fewer elective admissions were recorded the total economic value of the lower activity at the infected trusts during this time was £5.9 million.[35]

During the COVID-19 pandemic, unprecedented cybersecurity concerns related to emerged phishing attacks.[36] To give more details, a website very similar to the WHO'S internal email was developed by some hackers; the achievement they were looking for was to obtain credentials by stealing them from WHO workers.[37] [38]

In the Czech Republic on 12 March 2020 the Brno University Hospital had to close down its whole IT network. This developed consequences on different branches of the hospital such as the Children's Hospital and the Maternity Hospital.[39] It caused the necessity not only to delay urgent surgical interventions but also to redirect the new serious patients to a hospital close nearby. To retrieve the network, different groups collaborated to reach the goal, in particular teams from NCSC (the Czech National Cyber Security Centre), NCOZ (the Czech Police) and the IT staff from the hospital.[40]

Another example is what happened on 9 September 2020, when a ransomware hit the Düsseldorf University Hospital. Specifically, thirty servers were compromised, it was impossible to access patients' data and many of the medical equipment connected to the Wi-Fi were unavailable. In this confused

0.

[31] F. Donovan, *Judge Gives Final OK to $115M Anthem Data Breach Settlement*, in *Health IT Security*, 2018 available online at https://healthitsecurity.com/news/judge-gives-final-ok-to-115m-anthem-data-breach-settlement.

[32] J. Davis, *Anthem Settles with 44 States for $40M Over 2014 Breach of 78.8M*, in *HealthITSecurity*, 2020, available online at https://healthitsecurity.com/news/anthem-settles-with-44-states-for-40m-over-2014-breach78.8m?_cf_chl_tk=m1v9sXfqVLFDH4kcos62u_pecIqSFwpwVSvQmhjfz_I-1690222749-0-gaNycGzNDPs.

[33] T. Hofmann, *How organisations can ethically negotiate ransomware payments*, in *Network Security*, issue 10, 2020, 13-17, available online at https://digpath.co.uk/wpcontent/uploads/2020/10/NESE_2020-10_Oct.pdf.

[34] National Audit Office, *Investigation: WannaCry cyber-attack and the NHS*, 2017, available online at www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

[35] Ghafur, S., Kristensen, S., Honeyford, K. *et al*, *A retrospective impact analysis of the WannaCry cyberattack on the NHS*, in *Npj Digit. Med*, 2, 2019, 98, available online at www.nature.com/articles/s41746-019-0161-6#citeas.

[36] N. O'Brien, S. Ghafur, A. Sivaramakrishnan and M. Durkin, *Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that*, in *Digital Health*, vol. 8, 2022, 1-3.

[37] B. Kale, S. Aworo and C. Anyangwu, *Cyber-Attacks on Digital Infrastructures in HealthCare: The Secured Approach*, 2022, 1-12, available online at www.researchgate.net/publication/366323639.

[38] A.F. Al-Qahtani and S. Cresci, *The COVID-19 scamdemic: A survey of phishing attacks and their countermeasures during COVID-19*, in *IET Inf Secur*, vol. 16, issue 5, 2022, 324-345.

[39] F. Gioulekas, E. Stamatiadis, A. Tzikas, K. Gournaris, A. Georgiadou, A. Michalitsi-Psarrou, G. Doukas, M. Kontoulis, Y. Nikoloudakis, S. Marin, R. Cabecinha and C. Ntanos, *A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures*, in *Healthcare*, vol. 10, issue 2, 2022, 1-19.

[40] S. Parker and C. Mancarella, *Trust-IT, PANACEA Healthcare Cybersecuirity Advisory Services, COVID-19 is extending the cyber threat surface as healthcare organisations come under increasing strain*, 2020, available online at: www.panacearesearch.eu/watch/blog/covid-19-extending-cyber-threat-surface-healthcare-organisations-comeunder-increasing.

scenario there was a 78-year-old patient who was, due to a brain aneurysm, waiting for an emergency operation. The patient unfortunately died after the delay due to redirecting the ambulance to the Wuppertal Hospital.[41] [42]

Also, it is reported the first closure of an hospital related to a ransomware attack: the Saint Margaret's Health in the USA, occurred on 16 June 2023. The attack happened in 2021 and prevented the presentation of compensation's requests for months. The reported average cost to recover from a ransomware attack in the USA was 4,35 milions dollars.[43]

Another example is the Irish health system's IT infrastructure, which suffered a ransomware attack in May 2021. It impacted more than 80% of the system causing data theft and a hindrance to healthcare workers, who could not enter non clinical systems (such as finance and procurement) and clinical systems in order to give patients the required care. It took four months for the service to fully recover.

On August 2022, the Center Hospitalier Sud Francilien situated in Paris was hit by a ransomware attack and to obtain the decription key, the Center was required to pay $10,000,000.[44]

In 2022 Costa Rica suffered major ransomware attacks and for the first time a country has declared a "national emergency" in response to a cyberattack. According to the Costa Rican Social Security Fund the attack targeting Costa Rica's health care system at the end of May affected 484,215 medical appointments, needing massive rescheduling.[45]

The reported cases are only a selection of possible attacks, which can be grouped in the following classes.

1. Phishing by email;
2. Ransomware, which is "a malware that works by encrypting data saved in computers or the network itself. A ransomware attack is a malicious software that eliminates access to user data by encrypting" can be "cryptor" or "blocker". There are also "ransomware as a service (RaaS)", allowing to make a cyberattack to people without any specific knowledge.
3. Data loss or data theft.
4. Attacks to connected medical devices, considering that a medical device is defined as "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or another similar or related article, including a part or accessory, intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease".
5. Distributed-Denial-of-Service (DDoS).[46]

In the "2021 HIMSS Healthcare Cybersecurity Survey", "phishing" and "ransomware" are reported as the most frequent attacks.

According to the latest report by Europol, the cyber-attacks based on malwares are still the most prominent threat, with ransomware maintaining its position of the top threat. After the Russian attack against Ukraine, Distributed Denial of Service (DDoS) attacks against EU targets significantly increased.[47]

3. *Risks for patients in health structures*

Several factors make health care organizations attractive to would-be hackers, one being the economic value of data in the "*dark web*".[48]

Specific targets in the health information technologies (HIT) are:
- the electronic health records (EHR);
- the personal health records (PHR);
- the booking system for clinical appointments;
- the administrative system.

These targets are attractive for

[41] R. Shandler and M. A. Gomez, *The hidden threat of cyber-attacks – undermining public confidence in government*, in *Journal of Information Technology & Politics*, vol. 20, Issue 4, 2023, 359-374.
[42] A. Sunil Lekshmi, *Growing Concern on Healthcare Cyberattacks & Need for Cybersecurity*, 2022, 1-4.
[43] R. Patano, *Ransomware, le tecnologie avanzate per limitare i danni*, 2023. Available online at: www.agendadigitale.eu/sicurezza/ransomware-ecco-le-tecnologie-avanzate-per-limitare-i-danni.
[44] M. Horduna, S.-M. Lăzărescu and E. Simion, *A note on machine learning applied in ransomware detection*, in *Cryptology ePrint Archive*, 2023, 1-17.
[45] M. Burgess, *Conti's Attack Against Costa Rica Sparks a New Ransomware Era*, WIRED, 2022, available online at: www.wired.com/story/costa-rica-ransomware-conti.
[46] M.A. Ahmed, H.F. Sindi and M. Nour, *Cybersecurity in Hospitals: An Evaluation Model*, in *Cybersecurity and Privacy*, vol. 2, 2022, 854-855.
[47] Europol, *Europol Spotlight - Cyber-Attacks: The Apex Of Crime-as-a-Service*, 2023, available online at www.europol.europa.eu/cms/sites/default/files/documents/Spotlight%20Report%20-%20Cyber-attacks%20the%20apex%20of%20crime-as-a-service.pdf.
[48] S.T. Argaw *et al*., *The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review*, *op. cit*., 2.

cybercriminals: Personal Health Information (PHI) is bought and sold on the dark web for more than 10 times the amount of stolen credit card information, making it the most expensive data on the criminal market. The value is derived from the data points in the record that, when combined, can be used to create fake IDs, to buy medical equipment, write prescriptions and file false insurance claims. The multiple relationships, multiple touchpoint and multiple facilities of the industry make it susceptible to a variety of attacks. For example, a typical patient experience for an outpatient surgery can involve an initial encounter at the physician's office, an eligibility check with the insurance company, office contact to schedule the procedure, admission to the centre for surgery, and a pharmacy visit to have prescriptions filled.

The increased use of the "internet of medical things" devices, such as patient monitoring devices, which collect data, exchange data and are connected to the outside world, provides a major opportunity for security breaches. In addition, patients' growing demand for instant access to their data, combined with online scheduling capability, further exacerbates the challenge of ensuring the security of health care organizations' data systems.

From a medico-legal perspective, it is paramount to frame in a correct manner the issue regarding current cybercrimes targeting healthcare structures. If cybersecurity on one had is typically administered as a corporate tool for risk management as in for every enterprise in and beyond healthcare, in our digital era the access (or lack of) to data and the correct functioning of medical devices has become a major issue in administering Patient Safety. The issue is well known[49] [50] as a serious concern for Patient Safety operators.

One of the primary concerns in cybercrime prevention is the risk of unauthorized access to patient data. If healthcare systems are not properly secured, malicious individuals could gain unauthorized access to sensitive information such as medical history, diagnoses, treatment plans, and personal identifiers. This can lead to identity theft, fraud, or misuse of the data. Healthcare organizations store vast amounts of valuable data, making them attractive targets for cybercriminals. Data breaches can occur due to security vulnerabilities, human error, or sophisticated hacking techniques. When a breach happens, it can result in the exposure of sensitive patient information, leading to privacy violations and potential harm to patients.[51] [52] Data loss can occur due to hardware failures, software glitches, natural disasters, or cyberattacks. Inadequate backup systems or improper data management practices can lead to permanent loss of critical patient data, potentially impacting patient safety and continuity of care. It is also crucial to keep in mind that healthcare data is crucial for providing quality care and making informed medical decisions and that a delay on data availability or the impossibility to obtain certain information in critical occasion could led to serious (if not fatal) consequences for the patient. Ensuring secure data exchange and maintaining patient privacy during data sharing processes are critical challenges. In an interconnected healthcare ecosystem, sharing patient data across different systems and organizations is essential for coordinated care.[53] However, this also introduces potential vulnerabilities that require robust encryption methods, data access controls, and compliance with relevant regulations, especially considering that healthcare employees, contractors, or business associates with authorized access to patient data can also pose a security risk that may involve unauthorized use, disclosure, or modification of sensitive information for personal gain, revenge, or negligence.[54]

[49] L. Coventry and D. Branley, *Cybersecurity in healthcare: A narrative review of trends, threats and ways forward*, in *Maturitas*, vol. 113, 2018, 48-52. doi: 10.1016/j.maturitas.2018.04.008. Epub 2018 Apr 22. PMID: 29903648.

[50] C.S. Kruse, B. Frederick, T. Jacobson and D.K. Monticone, *Cybersecurity in healthcare: A systematic review of modern threats and trends*, in *Technol. Health Care*, vol. 25, issue 1, 2017, 1-10.

[51] A.H. Seh, M. Zarour, M. Alenezi, A.K. Sarkar, A. Agrawal, R. Kumar and R.A. Khan, *Healthcare Data Breaches: Insights and Implications*, in *Healthcare (Basel)*, vol. 8, no. 2, 13 May 2020, 133.

[52] A. Almalawi, A.I. Khan, F. Alsolami, Y.B. Abushark and A.S. Alfakeeh. *Managing Security of Healthcare Data for a Modern Healthcare System*, in *Sensors (Basel)*, vol. 23, no. 7, 30 Mar 2023, 3612.

[53] S. Canali, V. Schiaffonati and A. Aliverti, *Challenges and recommendations for wearable devices in digital health: Data quality, interoperability, health equity, fairness*, in *PLOS Digit Health*, 13 Oct 2022, vol. 1, no. e0000104.

[54] L.T. Martin, C. Nelson, D. Yeung, J.D. Acosta, N. Qureshi, T. Blagg, and A. Chandra, *The Issues of Interoperability and Data Connectedness for Public*

For all the aforementioned reasons healthcare data protection is subject to various legal and regulatory requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. Compliance with these regulations involves implementing technical and organizational measures to safeguard patient data, conducting risk assessments, and ensuring proper consent and authorization procedures. Addressing these concerns requires a multi-faceted approach, including implementing cybersecurity measures, conducting regular risk assessments, training staff on data protection protocols, establishing strong access controls, encrypting sensitive data, and ensuring regulatory compliance.[55]

Data protection is, therefore, a core duty of any health institution, to allow the appropriate cure of patients and to avoid secondary use of health information, which may expose the patient to legal (e.g., identity theft), economic or social (e.g., discrimination in health insurance or employment) negative consequences. Moreover, even when none is harmed by a data breach, there could still be deontological concerns.[56] The two major risks are represented by breach of confidentiality and breach of security. In the first case, the healthcare professional who received the personal information by the patient unlawfully discloses it to third parties. This scenario occurs not only when the information is transmitted without patient's consent, but more generally when there is no legal obligation to disclose confidential information. In this case, regulations and legal sanctions could be considered per se a proper response, being able to offset the risk. Instead, breach of security entails unauthorized access and/or use of personal information by people who were not involved in the physician-patient relationship. While the security of data generated by health care system, like those contained in health records, is heavily regulated, health-relevant data obtained through medical devices are generally considered to be more exposed to the risk of security breaches, especially in some countries.[57] Indeed, the regulatory frameworks largely vary among different countries, with European Union regulations generally considered broader than US sector-specific laws.[58] However, compliance with regulations (e.g., anonymization of data) does not mean to eradicate the risks for patients' privacy. For instance, GDPR and California Consumer Privacy Act require stringent criteria for data deidentification (since deidentified data are substantially no subject to regulation), but artificial intelligence can be able to reidentify information.[59] Therefore, health institutions must manage these risks implementing data security and access control measures.[60]

First, health institutions must limit data collection, ensure the minimalization, and must be always able to prove the equitability of the process (in order to contain specific risks, like that of biases).

Moreover, the data lifecycle must be clearly set and described, analyzing the risks of data leakage specific for any phase. That being said, access remains a crucial part of the process, being critical for both the user and the institution. Indeed, access to health services, including artificial intelligence products and wearables producing/storing/using sensitive data, is a core indicator of performance for health care systems.[61] Direct access to medical information is a legal right with a critical impact on patients' satisfaction, ability to recall and understand medical information,

Health, in *Big Data*, vol. 10, S1, 2022, S19-S24.

[55] E. Negro-Calduch, N. Azzopardi-Muscat, R.S. Krishnamurthy and D. Novillo-Ortiz, *Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews*, in *Int J Med Inform*, vol. 152, 2021, 104507.

[56] W.N. Prince 2nd and I.G. Cohen, *Privacy in the age of medical big data*, in *Nature Medicine*, vol. 25, issue 1, 2019, 37-43.

[57] D. McGraw and K.D. Mandl, *Privacy protections to encourage use of health-relevant digital data in a learning health system*, in *NPJ Digital Medicine*, vol. 4, 2021, Article number: 2.

[58] D. Grande, X. Luna Marti, R. Feuerstein-Simon, R.M. Merchant, D.A. Asch, A. Lewson and C.C. Cannuscio, *Health Policy and Privacy Challenges Associated With Digital Technology*, in *JAMA Network Open*, vol. 3, issue 7, 2020, e208285.

[59] B. Murdoch, *Privacy and artificial intelligence: challenges for protecting health information in a new era*, in *BMC Medical Ethics*, vol. 22, 2021, Article number: 122.

[60] K. Abouelmehdi, A. Beni-Hessane and H. Khaloufi, *Big healthcare data: preserving security and privacy*, in *Journal of Big Data*, vol. 5, issue 1, 2018, 1-8.

[61] J.F. Levesque, M.F. Harris and G. Russell, *Patient-centred access to health care: conceptualising access at the interface of health systems and populations*, in *International Journal for Equity in Health*, vol. 12, 2013, 1-9.

autonomy, and self-efficacy.[62] [63] Moreover, it is proven to increase organizational efficiency in health care facilities, also in particularly complex entities like mental institutions.[64]

Digital access is generally preferred by both healthcare professionals and patients, especially those facing barriers to healthcare access.[65] [66] Hence, specific policies must be implemented to address the risk of unauthorized digital access to information, designing safe authentication processes, encrypting/masking sensitive data to avoid unauthorized accesses, and governing accesses in compliance with an access control policy specifying privileges and rights of each authorized user (e.g., creating health data access level categories based on the trustworthiness of the user).[67] Finally, fostering effective patients-institution communication (aimed at increasing the transparency of the processes) and education of the healthcare professionals, who should be aware that the use even of deidentified data is never a zero-risk operation, are key interventions.

Regarding the risks, they are not limited to "internal failures" (e.g., unauthorized access to digital infrastructure of the institution) but also to external attacks, like ransomware attacks.[68]

The examples reported in this article show how ransomware attacks expose a significantly higher share of patients to the threat of data breach and can have catastrophic implications also in terms of patient safety (e.g., external control over medical devices/inhibited care due to disruptions), reputational damages and compensations/penalties caused by direct damages and failure to meet regulations.[69] In these cases, root cause analysis is often jeopardized by poor quality/quantity of data regarding attacks: indeed, hospitals usually are not compelled to report all the operational disruptions and they fail to do so especially when the event did not cause a direct harm for the patient. Addressing this threat in a multidisciplinary way (combining technical and medical expertise) should be seen as a public health priority, since cyber threats can jeopardize entire healthcare networks, propagating or even through the sole subsequent operational downtimes.[70] Ignoring the exact frequency and sophistication of the phenomenon exposes healthcare institutions and decision-makers to the risk of developing inappropriate responses or failing to develop responses to this growing issue. On the other side, an exact awareness of the issue means enabling decision-makers to tailor technical interventions and empowering safety culture among healthcare personnel.

In general, the spectrum of potential vulnerabilities and then the spectrum of potential interventions are broad. The main cause of events is represented by the human error (e.g., opening a phishing email), whose likelihood in turn can be boosted by preventable organizational factors such as excessive workload and reduced in case of proper training. Low awareness of cyber risks and of their implications is also another critical factor, also because it entails other risk factors like poor budgeting. Moreover, some radical changes (enhanced by the COVID-19 pandemic) in the work routine can influence

[62] S.E. Ross and C.T. Lin, *The effects of promoting patient access to medical records: a review*, in *Journal of the American Medical Informatics Association*, vol. 10, issue 2, 2003, 129-138.
[63] B. Fisher, V. Bhavnani and M. Winfield, *How patients use access to their full health records: a qualitative study of patients in general practice*, in *Journal of the Royal Society of Medicine*, vol. 102, issue 12, 2009, 539-544.
[64] A. Tapuria, T. Porat, D. Kalra, G. Dsouza, S. Xiaohui, and V. Curcin, Im*pact of patient access to their electronic health record: systematic review*, in *Informatics for Health and Social Care*, vol. 46, issue 2, 2021, 194-206.
[65] A. Scantlebury, A. Booth and B. Hanley, *Experiences, practices and barriers to accessing health information: A qualitative study*, in *International Journal of Medical Informatics*, vol. 103, 2017, 103-108.
[66] N. Bhandari, Y. Shi and K. Jung, *Seeking health information online: does limited healthcare access matter?*, in *Journal of the American Medical Informatics Association*, vol. 21, issue 6, 2014, 1113-1117.
[67] D. Xiang and W. Cai, *Privacy Protection and Secondary Use of Health Data: Strategies and Methods*, in *BioMed Research International*, vol. 2021, 2021, Article ID 6967166.
[68] H.T. Neprash, C.C. McGlave, D.A. Cross, B.A. Virnig, M.A. Puskarich, J.D. Huling, A.Z. Rozenshtein and S.S. Nikpay, *Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations*, in *2016-2021 JAMA Health Forum*, vol. 3, issue 12, 2022, e224873-e224873.
[69] M. Evans, Y. He, L. Maglaras and H. Janicke, *HEART-IS: A novel technique for evaluating human error-related information security incidents*, in *Computers & Security*, vol. 80, 2019, 74-89.
[70] C. Dameff, J. Tully, T.C. Chan, E.M. Castillo, S. Savage, P. Maysent, T.M. Hemmen, B.J. Clay and C.A. Longhurst, *Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments,* in *the US*, in *Jama Network Open*, vol. 6, issue 5, 2023, e2312270-e2312270.

the cyber risks: for instance, remote work (e.g., telemedicine) exposed the network to additional vulnerabilities, especially when unprotected wireless connections are used. Finally, inadequate protection of endpoint devices (e.g., laptops, medical devices) can represent an unprotected entry point for external attacks. As said, proper interventions require a combined and coordinated approach that includes IT resources and risk management experts. Indeed, besides technical interventions (e.g., secure remote work environment, regular software updates, creation of strong passwords, appropriate user authentication and data encryption), education (e.g., promotion of cyber culture) and management of human errors are crucial.[71] [72] Methods of human reliability analysis encompassing proper incident reporting and sharing processes have been recommended for dealing with human errors. For instance, Evans et al. proposed a combined mapping/analysis method (HEART-IS: Human Error Assessment and Reduction Technique of Information Security) to allow for root cause analysis and in particular to classify the human error (e.g., distinguishing omissive from commissive conducts), obtain descriptive information (e.g., role and frequency of the task that led to the error), and analyze all the error producing conditions (i.e., the conditions that could have increased the risks of error).

It is worth mentioning and underlining, once more, that the potential risks for patients due to cybercrime are not just damages related to privacy issues. The loss of data or the inoperability of a network or a medical device can lead directly (in medico-legal terms without the interruption of the causal link, meaning full liability on behalf of the Healthcare Enterprise) to a threat to the actual health of a patient and consequently biological damage (including certainly fatal events) that will require evaluation and compensation. The transposition of a digital risk to a very practical problem with physical consequences just mirrors our society's interdependence from digital devices and data, and ignoring such link represents a huge liability and vulnerability for every kind of healthcare structure. As in many other health-related areas concerning both risk management and patient safety, a more integrated approach would be preferable. A stricter collaboration with an approach that encompasses both cybersecurity and a more medico-legal perspective with an evaluation of threats and potential damages could lead towards a safer environment and a more conscientious use of digital data and devices from healthcare professionals.

The *"Healthcare Cybersecurity"* study by "*Bitdefender*", presented at the "*Healthcare Security Summit 2021 of Clusit*" pinpointed the following critical points:

- operating systems expired or not updated;
- inadequate protection of medical devices;
- no continuous control of risks of cyberattacks;
- too few specialists;
- inadequate funding compared to the threads.[73]

The situation will be more and more difficult to handle with the internet of medical things, allowing immediate data exchange. The development of the new resulting cyber ecosystems implies new cyber-risks.[74]

In Europe the situation is differentiated country by country in term of health systems. Italy, Finland and Sweden followed different path in national and regional policies about e-Health between 2009 and 2019.[75] Germany used resources from the Recovery and Resilience Plan for public health services, including digital infrastructure, telemedicine and information technology and cybersecurity.[76] A World Health Organization Europe project about health system transformation compared three European

[71] Y. He, A. Aliyu, M. Evans and C. Luo, *Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review*, in *Journal of Medical Internet Research*, vol. 23, issue 4, 2021, e21747.

[72] J.G. Ronquillo, J. Erik Winterholler, K. Cwikla, R. Szymanski and C. Levy, *Health IT, hacking, and cybersecurity: national trends in data breaches of protected health information*, in *JAMIA Open*, vol. 1, issue 1, 2018, 15-19.

[73] Agenda Digitale, *Sanità italiana nel mirino del cybercrime: grosso guaio per tutti i pazienti*, 2022, available online at www.agendadigitale.eu/sicurezza/sanita-nel-mirino-del-cyber-crime-cosi-litalia-rischia-grosso

[74] M.E. Watkins, D*esigning an Effective Organizational Culture to Guard Against the Cyber Risks of Emerging Technologies*, in *Journal of Healthcare Management*, vol. 68, issue 4, 2023, 239-250.

[75] H. Valokivi, S. Carlo, E. Kvist and M. Outila, *Digital ageing in Europe: a comparative analysis of Italian, Finnish and Swedish national policies on eHealth*, in *Ageing and Society*, vol. 43, issue 4, 2023, 835-856.

[76] European Commission, *State of Health in the EU: Synthesis Report 2023*, 2023, available online at https://health.ec.europa.eu/system/files/2023-12/state_2023_synthesis-report_en.pdf.

countries: Portugal, Sweden and UK. If on one hand in Portugal legislation is seen as an essential tool, on the other hand in Sweden and the UK legal means alone are considered insufficient for improving health systems.[77]

If the same legal approach cannot be followed neither all over Europe nor in a single country as Italy, where the health administration responsibility is shared between the central government and the different regions, approaches based on standards can be more appropriate.

A fruitful support to risk management is the ISO 31000 standard, published in 2009 and updated in 2018. It is a guideline for organizations that adopt a risk management model, based on fundamental principles. The first is an orientation towards continuous improvement. Others are to be dynamic and adaptable to evolving scenarios and enhance and build on the skills and knowledge of the human resources involved in functions and processes.[78] The model proposed by the ISO 31000 standard is based on risk assessment and risk treatment.[79] According to Ferdosi et al. risk evaluation in healthcare organizations must include the comparison of the results of the risk analysis with the risk evaluation criteria defined during the context establishment to determine whether the cyber-risks are acceptable.[80]

Healthcare sector is nowadays very concerned with clinical risks but cyber-risks are becoming more and more important not only because of the legal consequences due to the misuse of the data of patients but also because the cyber-attacks can prevent health organizations from treating their patients.

4. *Conclusion*

Health information storage and security have been revolutionized by information technologies for the last decades, going from handwritten notes to "immaterial" data stored in interconnected devices and/or in logical pools ("clouds"). This revolution amplifies the meaning and the complexity of the term privacy, also exposing health institutions to new kinds of vulnerabilities. Regulations are key interventions in this context, with supernational entities like European Union having a common, broad and complex framework (GDPR) and – in general – a significant disparity among the countries in the world. However, addressing these threats cannot be solely based on legal means, since a fruitful approach should include also IT and risk management strategies, together with the compliance with standards such as ISO 31000. Prevention and management of cyber-risk in healthcare requires a multidisciplinary approach; in our digital culture healthcare professionals (as well as administrative staff involved in healthcare) need to be trained specifically in cyber security in order to avoid damages. Therefore, is nowadays anachronistic to assume that a Medical Expert may be just proficient in medicine in order to perform a correct service in management of a healthcare organisation and a solid digital expertise should be required for healthcare experts who work in central structures and who device operative working procedures.

[77] D.J. Hunter and R. Bengoa*, Meeting the challenge of health system transformation,* in *European countries*, in *Policy and Society*, vol. 42, issue 1, 2023, 14–27.
[78] B. Gaudenzi, *Il Risk Management nelle aziende sanitarie*, in *Rivista Italiana di Medicina Legale e del Diritto in Campo Sanitario*, vol. 4, 2020, 1997-2011.
[79] ISO (2009) International standard: risk management: principles and guidelines. ISO 31000. Principes Et Lignes Directrices. ISO.
[80] M. Ferdosi, R. Rezayatmand and Y. Molavi Taleghani, *Risk Management in Executive Levels of Healthcare Organizations: Insights from a Scoping Review (2018)*, in *Risk Manag. Health Policy*, vol. 13, 2020, 215-243.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 299-306
ISSN 2724-5969 – ISBN 979-12-2181-128-5 – DOI 10.53136/9791221811285 24

*Artificial Intelligence as a Strategic Opportunity to Rearrange and Renew Public Management**

Rocío Navarro González
(Professor of Administrative Law at San Pablo Olavide University)

ABSTRACT Technological progress has been running parallel to the development of different paradigms in public management. The current context of emerging technologies allows Public Administrations to initiate a holistic process of comprehensive innovation to organise and renew the different management models used in Public Administration along with the internal decision-making mechanisms. Artificial intelligence offers a strategic opportunity in public management to strengthen decision-making and capacity for action by modernising structures and management mechanisms within Public Administration.

1. *Introduction*

The current technological revolution is transforming the economic model, the political system, the labour market, social organisation and even patterns of behaviour in our society. The overwhelming pace of technological changes since the beginning of this century is generating a new kind of society: the fourth industrial revolution.

These technological advances brought about by the revolution 4.0 represent a great opportunity for major public institutions such as Public Administrations to solve the majority of their conceptual and organisational problems. In addition to this, Administrations are finding that they are increasingly lacking protagonism in the context of governance compared to new social actors such as enterprises and social movements, which diminishe a large part of their institutional legitimacy.

With the arrival of new information and communication technologies (ICTs) and the roll-out of e-Administration, an optimal relationship has been attained between such institutions and citizens by improving Administration front-offices. In addition, ICTs have contributed to the achievement of greater equity in the provision of public services and to favouring systems of participation in public decision-making. However, other relevant aspects and issues relating to the management model and administrative efficiency have remained unchanged. Everything related to the back-office has not experienced any significant improvements or change.

The digitisation of Public Administration provides a climate that is conducive to innovation, harnessing the new technological paradigm to organise different management models for Public Administration and reduce the current legitimacy deficit through higher levels of institutional quality.

The current context of emerging technologies offers a new opportunity for Public Administrations to innovate holistically to improve both internal decision-making mechanisms and public-management models. Artificial intelligence as a strategy could fuel the exponential growth of a more collaborative and citizen-oriented Public Administration.

2. *Technological advances and their impact on the public sector*

In recent decades, reforms of institutional organisations have been marked by different events such as the development of technology, political changes, and the economic and financial crisis. In countries around us, Public Administrations have not maintained a passive and invariable stance.

One example of this is Poland. In Poland, from 1990 onwards, there was the greatest transition in terms of powers from a centralised authoritarian state after the communist regime to a system of local self-government. The introduction of a Local Government Law brought about significant administrative reform promoted by Regulski among others.[1]

Spanish doctrine, on the other hand, argues

* Article submitted to double-blind peer review.

[1] P. Swianiewicz, *Local government in Poland: the transition from a centralised authoritarian State to the system of local self-government,* Diputación de Barcelona, Barcelona, 2006.

that there have been no genuine reformation processes but rather a modernisation of fundamental aspects of the Administration related to public management, seeking efficiency or administrative quality.[2] The different measures and legislative reforms adopted have not affected the structural core of the Public Administration but have allowed for the implementation of new information and communication technologies (ICTs).[3]

With the technological revolution that began in the 1950s, the Public Administration has reconsidered the need to adapt to new technologies and initiated a new process of administrative modernisation with the automation and computerisation of administrative activity. Over this last decade, with the explosion of the Internet, new information technologies are generating technological innovations with a major social and economic impact such as Big Data, artificial intelligence, 3D printing, the Internet of Things and robotics, among others. This technological revolution represents a great opportunity to regenerate the Public Administration with a profound transformation that is significant enough to bring about cultural and structural change.

One of the great challenges is related to digital transformation in the public sector because it represents a decisive leap in improving the effectiveness and efficiency of Public Administration, just as computerisation once did.

Digital administration is the result of a process of transformation within Public Administrations based on the innovative use of electronic media and disruptive technologies for the automation of activity and operations, openness to citizens, data collection and collaborative analysis, and the provision of digital services.[4] The incorporation into the public sector of disruptive technologies such as artificial intelligence and blockchain, among others, offers a new paradigm to consolidate the digitalisation of Public Administrations.

2.1. *European commitment to the digital transformation of the public sector: Spanish-Polish initiatives*

The European strategic agenda notes the interest of European institutions in digital transformation, promoting the right digital tools and finding financial support through Next Generation EU funds and the Multiannual Financial Framework.[5] In particular, the European Commission is immersed in the "Path to the Digital Decade" policy programme and has adopted different measures to maximise the benefits of digital transformation for all citizens, public administrations and companies in Europe. One example of this is Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme for the period 2021-2027, focusing particularly on ensuring that areas of public-sector interest relating to health, education and justice can deploy state-of-the-art digital technologies, such as artificial intelligence.[6]

In response to the digital policies set by the European Commission, the governments of the different member states are putting forward interesting proposals to promote digital transformation in different sectors of society.[7] Examples of this can be seen in both Poland and Spain.[8] Both countries presented their national artificial intelligence strategies: the National Artificial Intelligence Strategy (ENIA) in Spain, and the Policy for the development of artificial intelligence in Poland.[9]

[2] M. Arenilla, *Cuatro décadas de modernización vs reforma de la Administración Pública en España*, in *Methaodos. Revista de ciencias sociales*, no. 5 (2), 2017, 303; A. Nieto, *Un primer paso para la reforma de la Administración española*, INAP, 2013,163-183.

[3] Among others, the Modernisation Plan of the General State Administration (1992), the Modernisation Plan of Measures for the Improvement of Administration (2006-2008) and the CORA Report 2013.

[4] A. Cerrillo, *La transformación digital de la Administración Local*, Fundación Democracia y gobierno local, 2021.

[5] C.A. Ciaralli, *Condizionalità finanziaria, rule of law e dimensione (sovra)nazionale del conflitto*, in *Federalismi.it*, no. 16/2022, 80; N. Lupo, *Next Generation EU e sviluppi costituzionali dell'integrazione europea: verso un nuovo metodo di governo*, in *Diritto Pubblico*, fasc. 3, 2022, 729

[6] COM (2018) 434 final 2018/0227(COD).

[7] Understanding the digital development of a country involves monitoring and analysing a number of key indicators and trends https://goingdigital.oecd.org/countries/pol.

[8] The 2022 edition of the Digital Economy and Society Index (DESI) reflects the position of both countries: Spain ranks 7 out of the 27 EU Member States and Poland ranks 24 out of 27. However, between 2017 and 2022, Poland's aggregate DESI score grew slightly more than the EU average, indicating that Poland is catching up with the rest of the EU.

[9] OECD.AI (2021), promoted by EC/OECD (2021), National AI Policy Database, consulted on 6/6/2023,

The Polish public sector has undergone an advanced technological transformation in recent years. One of the government's priorities is the digitisation of Public Administration. The Polish government is working to harness the potential and risks of AI as one of its priorities. At the end of 2020, as part of Poland's national AI strategy, an important document entitled Policy for the development of artificial intelligence in Poland was approved by the Council of Ministers.[10] One of the strategic areas for the development of AI in Poland is the public sector, with strong interest in the roll-out of AI contracts, among other things. The document referred to above, as well as establishing the framework and basic principles for the deployment of AI technologies in Poland, includes a series of measures and targets in the short term (up to 2023), medium term (up to 2027) and long term (2027 onwards). Among the most immediate measures, there is concern to promote the use of unconventional public procurement modes more suited to the implementation of innovative solutions in the public sector.

In addition to planning activities, the government launched the GovTech Polska project in 2019 to find innovative technological and digital solutions that address the specific challenges of the Polish public sector. GovTech Polska is an institution that cooperates with the Polish government, and its area of activity is technological innovation in the public sector, including public procurement.

Spain's government, on the other hand, designs its action strategy through the Digital Spain Agenda 2025. Updated for the year 2026, this governmental measure sets out a series of actions and reforms structured into different strategic pillars.[11] One of these pillars refers to the digital transformation of the public sector that promotes the digitisation of public administrations at all levels and areas of action, especially employment, justice and social policies. In this strategic context, there is a Plan regarding the Recovery, Transformation and Resilience of the Spanish Economy that reiterates the commitment of the Spanish executive to digital transformation and is configured as a cross-cutting goal that grounds the different policies proposed, such as the modernisation of Public Administrations.[12] To further strengthen such measures, the 2021-2025 Digitalisation Plan for Public Administrations has been drawn up as a catalyst for technological innovation from the public sphere.[13] The Spanish strategy focuses particularly on promoting the use of AI in Public Administration with the creation of innovation labs for new services and applications in Public Administration (GobTechLab).

3. *The paradigm shift in public management*

Transformations in contemporary societies derived from technological advances have been running parallel to the development of different paradigms in public management. With the arrival of the new millennium, the management of contemporary Public Administrations is undergoing a process of change as a result of adaptation processes following the technological revolution. It is helpful to set out, even briefly, the evolution of management models to understand the role that new emerging technologies can play in the transformation of public management.

3.1 *Public management models*

Since the end of the 19th century, Public Administration has been channelled through various models inspired by the main currents of the moment: the client model, the bureaucratic model, the managerial model and the governance model.[14] The transition from one model to another has not been radical. Gradually and progressively, the Administration has been adapting to new

https://oecd.ai.

[10] Resolution no 196 of the Council of Ministers of 28 December 2020 on the establishment of the Policy for the development of artificial intelligence in Poland from 2020.

[11] The agenda has recently been revised incorporating two new cross-cutting pillars to promote impactful strategic projects through public-private partnerships (Strategic Projects for Economic Recovery and Transformation - PERTE) and the co-governance of State and Regional Government (Territorial Networks of Technological Specialisation - RETECH).

[12] Lever IV, on an Administration for the 21st Century, includes the 11th component: Modernisation of Public Administrations.

[13] Ministry of Economic Affairs and Digital Transformation, *Digitalisation Plan of Public Administrations 2021-2025. Digital Administration and Digital Public Services Strategy*, 1.

[14] For a more in-depth study of the different public management models, see M. Baena del Alcázar, *Manual de Ciencia de la Administración,* editorial síntesis, 2005, 87.

changes, incorporating the strategies and tools of each model. The different public-management models that have succeeded one another are not mutually exclusive. In Public Administration, several models can and in fact do coexist.

At first, the model that dominated until just over a century ago was the client model that responded to the natural logic of any organisation by resorting to networks of family and friends. Present in most Western countries, it is considered harmful to public institutions due to shortcomings such as arbitrariness, clientelism and corruption. In order to alleviate such anomalies, a second model designed by Weber appears, more rigid and neutral than the previous one, based largely on meritocracy. Although this model provides a value of great importance to achieve economic development, and institutional and legal security, it hinders the flexible and effective provision of services. It is the organisational paradigm of modern society focused on rationality and legality and ties in with the modern State.

In the late 80s, with Anglo-Saxon influences, the managerial model emerges, following the current of New Public Management. It is a flexible model with an economistic vision that focuses on the effectiveness and efficiency of public organisations and on privatisation proposals for public services. For this model, public management improves when managers have some discretion and flexibility with the use of resources to carry out their responsibilities. But this model weakens the State by forgetting public principles and institutional values.

At this time, a new model appears with the need to build collaboration networks with public-private actors to solve social problems. The complexity of actors and problems linked to the defence of the common good and general interest cannot be resolved exclusively by public authorities. Companies, citizens and social movements must also be engaged and collaborate through technology-based social networks. This governance model is a plural model that calls for balance between efficiency and democratic participation with a more open, participatory and collaborative way of governing. This model is based on the idea that legitimacy is achieved not only by being effective and efficient but also with the democratic element that combines transparency or participation.

Although both the Weberian model and the managerial model are the two great paradigms of public management, there is no one dominant model. There is no prevalent pure model. Rather, in a somewhat disorderly way, Public Administrations operate under a mixture of models in which one can glimpse "a bureaucratic culture with a managerial culture of efficiency and business inspiration".[15]

Since the mid-2010s, new collaborative dynamics involving social actors in the process of public decision-making with the new generation of technologies and social media have sparked doctrinal proposals about new paradigms.[16] These proposals aim to combine both legal and institutional security with innovation capacity and flexibility to achieve effectiveness and efficiency in the context of this new society. This bureau-business model is an orderly mix between the bureaucratic model and the managerial model that combines business practices with public values.[17] It is evident that all these technological advances and the changes they generate are once again affecting the course of contemporary public management with a more complex governance model that adds in citizen participation, co-management of services, collaborative systems and public-private partnerships.

3.2 *The interaction of ICTs in public management*

ICTs have transformative potential within Public Administration, and this affects the evolution of public management, as the doctrine has shown.[18] Despite the reluctance reflected in the relationship between public

[15] C. Ramió, *Inteligencia artificial y Administración Pública. Robots y humanos compartiendo el servicio público*, Madrid, Catarata, 2019, 35.

[16] J.I. Criado, *Nuevas tendencias en la Gestión Pública*, INAP, 2016, 36-37; C. Ramió, *La Administración pública del futuro. Instituciones, política, mercado y sociedad de la innovación,* Tecnos, 2017, 149.

[17] C. Ramió, *Inteligencia artificial y Administración Pública. Robots y humanos compartiendo el servicio público*, 144.

[18] C. Hood and H. Margetts, *The tools of Government in the Digital Age*, London, Palgrave, 2007; J.I. Criado and J.R. Gil, *Las tecnologías de la información y la Comunicación en las Administraciones Públicas contemporáneas*, in *Administración Pública y Tecnologías de la Información y Comunicación*, Mexico City, INFOTEC, 2016; J.I. Criado, *Entre sueños utópicos y visiones pesimistas,* Madrid, INAP, 2009.

management and ICTs in the past, Public Administrations have gradually adopted technologies in the different phases of technological innovation.

During the consolidation of the bureaucratic model, information technologies supplanted certain internal management activities. The use of ICT was limited to automating tasks. Then, during the new public management stage, a period of computerisation began in the public sector. With the arrival of new applications derived from the Internet and web pages, ICTs have been used to digitise and achieve efficiency focused on an economistic vision to optimise internal processes and reduce administrative burdens.

In line with public governance, new digital technologies and communication systems facilitate public-sector collaboration with new actors through online services and interoperability between Public Administrations.

Therefore, the interaction of ICT and public management is of particular importance to understand the current public management paradigm. The role of new emerging technologies such as artificial intelligence is decisive in this new stage of technological innovation that is set to trigger a significant transformation in public management.

4. *Artificial intelligence and its impact on public administration management*

In Southern European countries, the use of artificial intelligence tools is less developed than in the United States, but in recent years their incorporation into the public sector is increasing. Within its lines of action, the European Union is prioritising the development of a specific and harmonised regulatory framework for artificial intelligence in all Member States in line with the vales and fundamental rights of the Union in order to achieve legal certainty. Europe understands the opportunities of the transformation this new emerging technology brings and of addressing its challenges through a common approach based around artificial intelligence. Of particular importance is the European Union White Paper on Artificial Intelligence: A European approach to excellence and trust[19] and the proposed Regulation of the European Parliament and the Council laying down harmonised rules for artificial intelligence - the Artificial Intelligence Act.[20] Europe is aware that in order to achieve levels of demand that support the development and adoption of artificial intelligence in the European Union's economy and public administration as a whole, it needs to step up its efforts at different levels. Among the proposals contained in the White Paper on artificial intelligence, in addition to supporting collaboration with other Member states and ensuring access to data and IT infrastructures, it emphasises the need for public sectors to adopt artificial intelligence. Specifically, one of the actions included, Action 6, states: "The Commission will initiate open and transparent sector dialogues giving priority to healthcare, rural administrations and public-service operators in order to present an action plan to facilitate development, experimentation and adoption." It then notes that: "The sector dialogues will be used to prepare a specific 'Adopt AI programme' that will support public procurement of AI systems, and help to transform public procurement processes themselves."

As pointed out previously, both the Spanish and the Polish states, aligned with the European Digital Agenda, present their own strategies for the development of sustainable artificial intelligence, focused on citizenship: the National Artificial Intelligence Strategy (ENIA) in Spain, and the Policy for the development of artificial intelligence in Poland. EU Public Administrations are increasingly exploring the application of artificial intelligence to improve public services, the formulation of policies and internal management since there is no doubt that artificial intelligence could potentially

[19] Communication from the European Commission COM (2020) 65 final, of 19 February. The White Paper calls to establish both a policy framework to mobilise resources through public-private collaboration and an ecosystem of excellence, as well as a regulatory framework for artificial intelligence that generates an ecosystem of trust, respecting the values and rights of citizens of the European Union (EU). Two particularly relevant communications on artificial intelligence were previously adopted: The Communication from the European Commission on Artificial Intelligence for Europe COM (2018) 237 of 27 April and the Coordinated Plan on Artificial Intelligence, Communication of the European Commission COM (2018) 795 of 7 December.

[20] COM/2021/206 final, of 21 April. For a detailed analysis of both the White Paper and the proposed regulation, see E. Gamero, *El enfoque europeo de inteligencia artificial*, in *Revista de Derecho Administrativo*, no. 20, 2021, 268-289.

improve public management and the effective functioning of Public Administrations in public decision-making and service provision. Of particular interest are the AI Watch reports produced by the European Commission, which reflect results and comparative studies on the potential of artificial intelligence in the public sector.[21]

The economic growth and social well-being of today's society uses values created by consumer data, which are stored and processed mostly in infrastructures located in centralised clouds. In the near future, the data will come from industry, business and the public sector and will be stored in different systems, including computing devices operating at the edge of the network. Artificial intelligence, as a combination of technologies that groups data, algorithms and computing capacity, presents a very significant option. Artificial intelligence is, in turn, one of the most important parts of the data economy.

Artificial intelligence is based on the use of algorithms and data. The use of quality data through algorithms can facilitate such decisions and the provision of public services, improving the performance and outcomes of administrative activity. Therefore, Public Administrations should not hesitate to increase institutional capacities in data governance as a preliminary step to implementing artificial intelligence, establishing responsibilities in decision-making and guidelines to consolidate quality and the appropriate use of data. We saw previously how Public Administrations have adopted acts or developed actions through electronic means without the direct intervention of the people. The automation process has evolved as media have become technologically more advanced. Artificial intelligence is currently being used in automated administrative actions. One question that is open to debate is which decisions can be automated, and whether there are public decisions which require human intervention.[22]

There is consensus that the use of artificial intelligence allows for the automation of regulated decision-making, but the potential offered by artificial intelligence points to the possibility that Public Administrations can automate discretionary decision-making. All this taking into account the general principle of precaution for discretionary decisions, needing to assess, among other things, the type of decision, the environment in which it should be made, and the availability of data.[23] Public Administrations are progressively using algorithms and incorporating bots to automate actions.

Artificial intelligence could also offer a great opportunity to implement an institutional and organisational renewal of Public Administration and contribute to its adaptation in a context in which the paradigm of governance coexists with other management models.

All the technological advances developed over the last four decades have had an impact on public management. Hence, the arrival of emerging technologies such as artificial intelligence makes us think that there will be a radical transformation in public management with repercussions in terms of its models. The new model must strike a balance between old and new paradigms, allowing a hybrid system to emerge, as some authors have already ventured.[24]

The disparity of competences and diversity of activities carried out by Public Administration prevents us from relocating all its activity within a single model, separating it out from the rest. The coexistence of both models is possible and also advisable given the diversity of administrative activities. For activities pertaining to the regulation of rights, the bureaucratic model would be a better fit, whereas the managerial model would be more in keeping with the provision of services. However, for all possible public-private partnerships, the governance model would be required.

Artificial intelligence presents a great opportunity to rearrange the different

[21] https://ai-watch.ec.europa.eu/index_en.

[22] J. Valero, *El régimen jurídico de la e-Administración,* Granada, Comares, 2007; I. Alamillo and X. Urios, *La actuación administrativa automatizada en el ámbito de las Administraciones Públicas. Análisis jurídico y metodológico para la construcción y explotación de trámites automáticos*, Escuela de Administración Pública de Catalunya, 2011; J. Ponce, *Inteligencia artificial, derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo tecnológico*, in *Revista General de Derecho Administrativo*, no. 50, 2019.

[23] A. Cerrillo, *Actividad administrativa automatizada y utilización de algoritmos*, in (AAVV) *Las políticas de buen gobierno en Andalucía (I): Digitalización y Transparencia,* Instituto Andaluz de Administración Pública, 2022, 259-287.

[24] C. Ramió, *Innovación pública en Iberoamérica: presente y tendencias de futuro*, CLAD, 2021.

management models within the pre-eminent governance model. Artificial intelligence would allow us to definitively achieve, as the doctrine has shown, a solid, objective, neutral and effective bureaucratic model impervious to clientelism and corruption with higher levels of legal certainty through the automation of processes. We must be on alert so that artificial intelligence algorithms do not give rise to mathematical management with consequences in terms of political patronage. There are proposals for Public Administrations to have artificial intelligence programmes of neutrality and equity that are responsible for validating the other algorithms and artificial intelligence programmes. In turn, artificial intelligence in the management model would benefit areas of the Administration that provide public services such as social services, health and education, by achieving greater effectiveness and efficiency. Finally, in a scenario of public-private collaboration, the intensive use of artificial intelligence by Public Administrations would ensure the possibility of planning, controlling and evaluating private organisations that deliver public services.

Doctrinally, one predicted vector of change in 2020-2030 is the possibility of anticipating a radical shift in management models linked to digital administration and the introduction of artificial intelligence in public management.[25] This task will require both innovative thinking to anticipate the multiple impacts and the reflection of such issues in public debate. The doctrine considers that the traditional dynamics of modernisation and innovation in Public Administrations will have to be renewed and thus achieve modern, solid public institutions that adapt to the possible changes that will mark the 21st century. And in the design of such institutions, a strategy of technological renewal linked to AI and robotics is necessary.

Public Administration must not be reactive to management innovation through artificial intelligence; it must be opened up, as indicated by the Ibero-American Charter for innovation in public management, to possibilities in the improvement and economic sustainability of public services offered by the implementation of artificial intelligence in favour of the common good and general interest.[26] The same text expressly points out in its Preamble that Public Administrations are "innovative agents that are continuously transforming and expanding the policies and public services they provide to citizens according to their new demands and needs".

Within the current digitalisation of Public Administration, a favourable climate for the promotion of innovation is being created, where artificial intelligence is a key element to achieve such innovation in public management. Undeniably, the incorporation of artificial intelligence into the public sector gives way to a new model of Public Administration based on data analysis.

Artificial intelligence like the other technological developments that characterise the exponential era -cryptocurrencies, big data, internet of things, driver-less cars ...- generate a series of impacts which should be anticipated through innovative thinking, managing to find a balance when faced with the challenges they present: extreme regulation, disincentivising technological change, or delaying it, so that effective and legitimate intervention comes too late.[27]

Issues of special importance are emerging at an astounding rate, eager for answers related to security and transparency, legal and ethical limits in the development of artificial intelligence that spark interest on the part of the European Union and the doctrine in the absence of a legal framework.[28] In particular, the use of tools based on artificial intelligence that we are seeing in the public sector to prevent corruption and fraud is significant.[29] We are seeing European initiatives such as the

[25] C. Ramió, *Innovación pública en Iberoamerica:presente y tendencias de futuro*, 30.

[26] The Charter was approved by the XIX Ibero-American Conference of Ministers of Public Administration and State Reform, held in Andorra on 8 October 2020.

[27] O. Oszlak, *Los impactos de la era exponencial sobre la gestión pública en los países emergentes,* in *Revista del CLAD Reforma y Democracia*, no. 76, 2020, 31.

[28] European Parliament resolution of 20 October 2020 with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies (2020/2012(INL); D. Kowalski, *Public economic law-current problems and challenges on examples of digitalization and robotization,* in Jagiello, S. Kursa and F. Parente, *Influence of information on the Legal System*, Difin, 2021, 188.

[29] O. Capdeferrro and J. Ponce*, Nudging e inteligencia artificial contra la corrupción en el sector público: posibilidades y riesgos, in Revista Digital del Derecho Administrativo*, issue 28, second semester, 2022, 225-258; J. Miranzo Diaz*, Inteligencia artificial y contratación pública*, I. Martin Delgado and J.A. Moreno Molina, *Administración electrónica, transparencia y contratación pública*, Madrid, Iustel, 2020, 105-142.

Arachne programme launched by the European Commission based on artificial intelligence, which analyses the risks of irregularities in the European funds management file, including the detection of previous irregularities such as convictions for corruption.

In short, the combination of digital design, big data and artificial intelligence can help improve the functioning of public management, thus promoting good administration, by improving legislative quality, transparency, and techniques for preventing corruption, among others. However, at the same time, adverse effects can arise that are offset by initiatives in different countries such as the Charter of Digital Rights.

5. *Conclusion*

Since the end of the 20th century, society has undergone important changes. The technological revolution spearheaded largely by information technologies has altered labour, economic, social and political parameters. Public administrations are aware, on the one hand, of a decline in their legitimacy, as deeply entrenched institutions associated with the role of the State, and, on the other, that they should not be pushed to the side lines in the work undertaken to adapt their organisation and their activity, faced with the transformations taking place in different areas of society.

Progressively, public administrations have been adapting technologies in the different phases of technological innovation. The role of ICTs has contributed to strengthening public institutions and achieving a high level of efficiency. So far, Public Administration has made use of digital instruments to transform the direct service provided to citizens, achieving satisfactory levels of effectiveness. With the new emerging technologies, it is a good time to renew the internal organisation of Public Administration and reorder the different management models applied.

Artificial intelligence is one of the technological innovations that champion the exponential era and contribute to the recovery of legitimacy within Public Administration through quality decision-making and service provision. The application of this technology would contribute to achieving improvements linked to the institutional back-office, both by renewing its management model and achieving a higher level of efficiency. This would deliver a governance model that engages organisations and citizens, a bureaucratic model that provides legal certainty, and a management model in the provision of quality public services. The implementation of technologies in the public sector paves the way for greater institutional quality and expands the scope of good governance and good administration

Interest in regulating and establishing a regulatory framework is still active and allows us to face the challenges that guarantee, among others, respect for fundamental rights, the assurance of transparency and security, always seeking a balance so as not to deter the implicit process of innovation. There are many varied challenges that arise in the academic horizon, and we must find answers for them, such as cybersecurity, interoperability, automated administrative activity, blockchain implementation, reliability, and legal and ethical limits.

Artificial intelligence is a useful and appropriate tool to implement an institutional renewal of Public Administrations that helps them to adapt in a complex context involving different actors. The objective is to go beyond simple digitisation and technological innovation and delve into the workings of management models to achieve greater institutional strength. With the improvements and advances brought by the implementation of new emerging technologies such as artificial intelligence, contemporary public management will embark on a change in direction.

By virtue of all this, this disruptive tool offers a strategic opportunity in public management to positively strengthen decision-making and the capacity for action by modernising structures and management mechanisms within Public Administration.

European Review of Digital Administration & Law - Erdal
2023, Volume 4, Issue 1, pp. 307-312
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 25

*More on Algorithms and Public Administration**

Alessandro Di Martino
(Assistant Professor of Administrative Law at University of Naples 'Federico II')

Tar Campania, Sez. III, 14 November 2022, n. 7003

The recourse to the algorithm within the administrative procedure can never involve a lowering of the level of procedural safeguards and, in particular, of the requirement to state reasons for the measure pursuant to Article 3 of Law 241 of 1990, which, on the contrary, in these cases appears reinforced.

ABSTRACT This paper analyses a recent judgement of the Campania Regional Administrative Court on algorithmic administration. The topic confirms its enduring relevance in the debate and returns to the relationship between discretion and binding nature in automated procedures. Moreover, the decision focuses on the principles necessary for a correct exercise of algorithmic administration, specifically the principle of knowability and non-exclusivity of the automated decision. Finally, the paper proposes a critical reading of the new Article 30 of the Public-Contracts Code, which is the first rule in the Italian frameword that expressly allows the use of artificial-intelligence instruments.

1. *Background, ruling and matters involved*

The T.A.R. Campania, with ruling no. 7003 of 2022,[1] returns once again to the issue of administration by algorithms, thus confirming its continuing relevance within the scientific debate.[2] Such issue concerns the allocation of a monetary indemnity for farms located in certain territories of Campania, intended for entrepreneurs to compensate for the additional costs and loss of income due to the location of agricultural land. Specifically, the Court calculated this indemnity based on two parameters (the altitude and the slope of the land), and Article 6 of the notices implementing those compensatory measures fully regulated the calculation procedure the algorithm used to calculate the measure. Having regard to an initial determination of the allowance, carried out with the algorithmic formula provided for in the notice, AGEA later deemed necessary to review the artificial-intelligence system based on the indications of the European Commission and, therefore, modified (in peius) the indemnities to correspond to farmers.

Basically, the administration introduced a different algorithm from the one set out in the call for tender, which led to a measure challenged by the applicant and declared unlawful by the administrative court for various procedural violations. First of all, the measure was unlawful because the administration did not indicate which new algorithm it had used, nor how it worked.

Moreover, the Campania Regional Administrative Court considered that the "recalculation" measure did not consider the guarantees of participation, that the decision had been adopted in breach of the call for tenders and, finally, that the new measures amounted to a revocation of the same, although there were no grounds to file an appeal pursuant to Article 21-quinquies.

The sequence of events allows the administrative judge to dwell once again on some of the principles underlying the proper use of computer algorithms and artificial-intelligence tools by public administrations. Indeed, the attention of the Campania Regional Administrative Court focuses on the centrality of the knowability principle of the algorithmic mechanism and on the principle of non-exclusivity of the automated decision (the so-called human in the loop).

* Article submitted to double-blind peer review.

[1] For a first comment on the judgement, see M. Sforna, *Le garanzie di conoscibilità degli algoritmi e l'esigenza di assicurare un controllo umano del procedimento amministrativo (c.d. human in the loop). Nota a Tar Campania, Sez. III, 14 novembre 2022, n. 7003*, in *www.giustizia-insieme.it*.

[2] The topic is investigated in a recent monographic volume by L. Torchia, *Lo Stato digitale*, Bologna, Il Mulino, 2023.

2. *The algorithms' extent in administrative proceedings: a move backwards towards 'low discretion'*

The decision mentioned above seems to take a slight step backwards with respect to the previous caselaw orientation on the scope of application of algorithms in administrative proceedings. Indeed, it is known that in judgments no. 8472 of 2019 and no. 881 of 2020, the Council of State extended the use of IT tools to all proceedings, both discretionary and otherwise (i.e., bound), through a balancing act that gave greater value to the 'advantages' underlying the use of algorithms.[3]

The idea that only so-called 'serial' procedures - i.e. bound procedures - could be automated was dismissed and, in contrast, an efficientist interpretation was stressed. Nevertheless, the Council of State's extensive interpretation of the two judgements caused several worries, especially regarding whether the machine can provide the same procedural guarantees that the 'human officer can provide through his/her balancing of interests.[4] Such an interpretation, for instance, makes democratic participation in fully automated procedures extremely complicated, since it would be complicated for the citizen to actually know the logic behind the machine and, therefore, to intervene in proactive or defensive terms.

The case law approach briefly referred to, again regarding the scope of the application of algorithms in administrative proceedings, is partially refuted by the ruling in comment, according to which recourse to algorithms - even in a partially decisional function - would be valid in serial proceedings, or in those characterised by "low discretion". The T.A.R. Campania's approach is certainly surprising because the previous position of the Council of State, besides appearing extremely solid, was more in line with the progressive evolution of new technologies;[5] however, the considerations expressed by the administrative judge are anything but innovative, since the admissibility of IT tools in proceedings with a low rate of discretion had already been discussed in the past.[6] In a nutshell, scholars' guidelines aimed to extend the automation of decision-making processes characterised by low discretionary power. Sihc approach moved from the need to temper the rigid assertions according to which entrusting the exercise of discretionary power to a computer could determine "a sort of ossification of administrative action" and lead to "a deindividualisation of the decision".[7] On the other hand, the administrative judge's decision deals with the subject in a different way, disregarding the perspective of administrative power and decision, but rather focusing on that of the citizen. Accordingly, the Campania Regional Administrative Court goes beyond the Council of State's approach and imposes a limit that public administrations cannot exceed, *i.e.* the "low discretion": the latter, constitutes the 'maximum admissible' in terms of guarantees, since the automation of decision-making processes "can never entail a lowering of the level of protection guaranteed by the law on administrative procedure, and in particular those on the identification of the person responsible for the procedure, on the obligation to state reasons, on the guarantees of participation, and on the so-called 'non-exclusivity' of algorithmic decisions".

3. *The algorithmic judge's lawfulness: the knowability principle*

Having specified the applicative scope of algorithmic administration, the judgement of the Campania Regional Administrative Court clarifies the hard core of principles underlying the use of IT tools by public administrations. First, public administrations are necessarily bound to comply with the principle of transparency of the automated decision. The latter, on deeper inspection, must be

[3] The commentaries on the judgements are several: above all, see A.G. Orofino and G. Gallone, *L'intelligenza artificiale al servizio delle funzioni amministrative: profili problematici e spunti di riflessione*, in *Giurisprudenza italiana*, 2020, 1738 ff.

[4] A. Di Martino, *Tecnica e potere nell'amministrazione per algoritmi*, Naples. Editoriale Scientifica, 2023.

[5] L. Previti, *La decisione amministrativa robotica,* Naples, Editoriale Scientifica, 2022, 192.

[6] A. Masucci, *L'atto amministrativo informatico*, Naples, Jovene, 1993; M. Natoli, *L'attività informatizzata della pubblica amministrazione*, in *Rivista amministrativa*, 2003, 960; recently, I.M. Delgado, *Automazione, intelligenza artificiale e pubblica amministrazione: vecchie categorie concettuali per nuovi problemi*?, in *Le istituzioni del federalismo*, 2019, 647; B. Marchetti, *La garanzia dello "human in the loop" alla prova della decisione amministrativa algoritmica*, in *BioLaw Journal*, 2021, 367 ff.

[7] See A. Contaldo and L. Marotta, *L'informatizzazione dell'atto amministrativo: cenni sulle problematiche in campo*, in *Il diritto dell'informazione e dell'informatica*, 2002, 571 ff.

understood in its four declinations of knowability, full knowledge, comprehension and control.[8] From the citizen's perspective, it is not enough to ensure the possibility of accessing the source code,[9] but it is necessary to guarantee the comprehension of all the technical steps that lead to that particular algorithmic decision. Setting this matter in the perspective of citizens' rights implies, on the other hand, a stronger duty to motivate on the part of the public administrations. The latter are obliged to translate the technical rule into a legal rule, in order to allow the addressees of the measure to grasp any illegitimacy profiles and, if necessary, to take legal action against the automated measure.[10]

The guarantee of the knowability of the algorithm, as it is well known, binds administrations not only through Article 1(1) of Law No. 241 of 1990, but also through Article 41 of the Charter of Fundamental Rights of the European Union. The latter states that when the public administration intends to adopt a decision that may have adverse effects on a person, it is obliged to hear the person before acting, to allow him/her access to its archives and documents, and to give reasons for its decisions. The assertions of scholarship and caselaw on the need to guarantee transparency in the decision-making process, even when automated, are undermined first and foremost by the technical complexity underlying the algorithm. For this reason, the issue does not only concern legal and procedural aspects, but (as the ruling of the Campania Regional Administrative Court confirms) also the technical, statistical, and engineering profiles of knowledge of the machine.

Another relevant aspect from the perspective of ensuring algorithm knowability is that of the type of computer tool used by the public administration. Indeed, it is very important to understand whether public administrations resort to deterministic algorithms, or whether they rely on artificial-intelligence tools (*machine learning*). In the case under comment, the calculation for the determination of the indemnity was performed by a deterministic algorithm; therefore, for its knowability, attention must be shifted to the construction of the algorithm and, above all, to the identification of the *inputs,* since the latter establish the moment in which the discretionary choice comes into play. However, scholarship pointed out that whenever public administrations resort to artificial-intelligence tools, it would be extremely complex to guarantee full and effective knowability of the decision-making process, since, very often, not even the programmers of the algorithm can understand the outcomes of the fully automated decision-making process.

3.1. *The principle of non-exclusivity of automated decision-making*

The judgement in comment addresses another extremely relevant aspect from the perspective of the legitimacy of automated decisions, namely the well-known principle of 'non-exclusivity of the algorithmic decision'. This is a rule confirming the 'instrumental', and not exclusively decisional, nature of algorithms and artificial intelligence tools for public administrations. From the citizen's perspective, 'algorithmic non-discrimination' takes the guise of a right in the strict sense, namely to not deciding solely by virtue of the automated process. On the other hand, on the administrative side, it implies the obligation for the person in charge of the procedure to check (validating or denying) the algorithmic decision.

The issue of (administrative, social and judicial) control of algorithmic decision-making is extremely complex and cannot be addressed in depth herein. However, it is an aspect that points to numerous limitations, both in terms of legitimacy and liability.

The limits on administrative and social control over automated administrative decisions clearly open a further and consubstantial problematic aspect, which concerns the identification of liability profiles of the public administration whenever it relies on an algorithm or an artificial-intelligence system to conduct administrative procedures.

In order to analyze the link between the effectiveness of the control power and the accountability of public administrations, it is

[8] According to the well-known reconstruction by G. Arena, *Trasparenza amministrativa,* in S. Cassese (ed.), *Dizionario di diritto amministrativo*, Milan, Giuffrè, 2006, 5945 ff.

[9] On this topic, see A.G. Orofino, *La trasparenza oltre la crisi*, Bari, Cacucci, 2020.

[10] Recently, scholarship has argued that it would be possible to make up for the procedural-participation deficit caused by the difficulty for citizens to intervene proactively or defensively in the automated procedure. In this sense, G. Gallone, *Riserva di umanità e funzioni amministrative*, Padua, Cedam, 2023.

necessary to retrieve the approaches of judgments n. 8479 of 2019 and n. 881 of 2020. Shortly after admitting the use of such IT tools in discretionary proceedings, the judgements take note of the problematic aspect relating to the imputation of the results of the administrative measure, stating that "in order to apply the general and traditional rules on imputability and liability, it is necessary to ensure that the final decision is referable to the authority and body competent under the law attributing the power".[11]

The administrative judge's referral is functional to recall the well-known principle of organic immedesimation,[12] a criterion of imputation of the (traditional) administrative act, which allows the acts and their effects as well as, more generally, the activity of its organs to be attributed directly to the legal person.

Before understanding whether it is possible to peg (bind) the administration by algorithms to a liability model compatible with those provided by the legal system, it seems necessary to understand whether public authorities, if they resort to the use of such pervasive computer tools, exercise a power to use it or not. In case of algorithms' deterministic use, *i.e.*, if a procedure is automated that is constrained insofar as it is hetero directed by law, it is a fairly well-established view that the public administration does not exercise power in the substantive sense. The unique valid perspective in the sense of a responsible administration in this sphere might seem to be whereby the power exercised by public offices would be found in the very choice of resorting to an automated procedure and, moreover, in the processes of 'educating' the algorithm.

On the other hand, organisational structures can also use self-learning algorithms, in which human input is completely *bypassed* even in the algorithm pre-determination phase. However, not even in this circumstance could it be said that power is concretely exercised, since the balancing-interest analysis is replaced by machine activity, making the figure of the person in charge of the procedure effectively obsolete.[13]

In proceedings conducted on the basis of a self-learning algorithm, not only would it not be possible to grasp that role that the legal system attributes to human person in the sense of being "the guide of the proceedings, the element of propulsion and coordination of the preliminary investigation and, correlatively, the sole interlocutor, a sure point of reference, of citizens in their relations with the administration".[14] But one could not even imagine the person in charge of the proceedings with the image formerly ideally portrayed by Frosini, by virtue of which he/she would perform the tasks of a "virtual official".[15] In these cases the machine behaves, in fact, in the same way as a 'human' official would behave and would be required to prepare a draft measure to be submitted to the manager of the organisational unit that, at least in a theory, would remain responsible for the decision taken.[16]

However, the traditional regime of public administration liability collapses when the latter uses artificial-intelligence tools. Due to the difficulty of controlling the output of the algorithm, which stems from the digital divide of civil servants.[17]

In fact, the use of *machine learning* would make the figure outlined in Articles 5-6 of Law No. 241 of 1990 completely useless, since it would not be possible to understand how the person involved in the proceedings would be able, for instance, to ascertain the facts *ex officio* and adopt each measure for the proper and prompt conduct of the investigation', since the prompt (and complete) conduct of the investigation should be guaranteed by the algorithm.

[11] Cons. Stato, Sez. VI, 4 February 2020, no. 881, point 10.6.

[12] On the subject, most recently, M.C. Cavallaro, *Immedesimazione organica e criteri di imputazione della responsabilità*, in *Persona e amministrazione*, 2019, pp. 39 ff.

[13] D. Donati, *Digital divide e promozione della diffusione delle ICT*, in F. Merloni (ed.), *Introduzione all'e-government: pubbliche amministrazioni e società dell'informazione*, Turin, Giappichelli, 2005, pp. 209 ff.

[14] M. Immordino, M.C. Cavallaro and N. Gullo, *Il responsabile del procedimento*, in M.A. Sandulli (ed.), *Codice dell'azione amministrativa,* Milan, Giuffrè, 2017, p. 550.

[15] V. Frosini, *L'informatica e la pubblica amministrazione,* in *Rivista trimestrale di diritto pubblica.*, 1983, 484.

[16] In this sense, A.G. Orofino and R.G. Orofino, *L'automazione amministrativa: imputazione e responsabilità*, in *Giornale di diritto amministrativo*, 2005, p. 1311, as well as M.C. Cavallaro, *Imputazione e responsabilità*, 72.

[17] As recently argued by V. Neri, *Diritto amministrativo e intelligenza artificiale: un amore possibile*, in *Urbanistica e appalti*, 2021, p. 592; but, in these terms, M.C. Cavallaro, *Imputazione e responsabilità*, 72-73.

However, the main issue to be resolved concerns the possibility for the body responsible for the adoption of the final measure to depart from the results of the preliminary investigation conducted by the *virtual procedural officer* by providing an adequate justification.

In this context, it appears (or, rather, re-appears) without any doubt an intense relationship between the principles of accountability and transparency and the obligation to state reasons to adopt a different measure by not deeming valid the conclusions reached during the preliminary investigation. Indeed, it would be extremely complex for anybody responsible for the adoption of the final measure to grasp the dynamics underlying the self-learning algorithm, where, precisely in these circumstances, one is in the presence of computer tools that are so 'autonomous' that not even the programmers are sometimes able to grasp all the steps that the machine has followed. Once again, transparency could be the key to resolution, since it creates a link with the administration's responsibility to demonstrate that the *input* provided and the operation of the algorithm conforms to the reasonableness[18] parameters imposed by the law.[19]

The intrinsic difficulty regarding recourse to such computerised tools highlights another complex profile, following from the full knowledge of algorithmic dynamics. This aspect has already been mentioned, nevertheless deserves to be deeply analyzed to assess the inapplicability of the procedural rules dictated by Article 6 of Law No. 241 of 1990. Would it really be conceivable for the body responsible to adopt the final measure to provide adequate justification for its intention not to comply with the findings of the automated preliminary investigation, where it does not have the technical tools to be able to understand the 'reasons of the machine'?

The answer is certainly negative and recalls the more general role of new techniques in the decision-making processes of public administrations and the role of the competences of bureaucratic apparatuses.

In fact, only where 'administrators' will be able to cope with the evolution and progress of computer techniques, will the use of algorithms in decision-making processes constitute a tool for the best pursuit of the public interest, thus making rules such as those in Article 6 of the General Law on Administrative Procedure applicable and relevant again. If this is not the case, i.e. if we continue not to invest in the quantitative and qualitative increase of the staffing of public servants, human intellectual input will have less and less impact than technical input, which will become predominant in every phase of the administrative decision-making process and which will certainly not allow the traditional person in charge of the procedure to correct and improve the preliminary investigation conducted by the algorithm and consequently, carry out a full and effective control over the correctness of the IT tool, which could lead to the actual legitimisation of the administrative-function exercise in specific circumstances.

4. *From caselaw legality to substantive legality: the new Article 30 of the Public Contracts Code*

It has been said so far that the algorithmic administration bases its foundations on the principles laid down by case law, in the perspective of a so-called 'algorithmic legality', with no relevance whatsoever to the provision of Article *3-bis* of Law No. 241 of 1990.

The relevant scope of the discussion on the *breach of* substantive legality, filled by a 'procedural' legality, was grasped by the legislator. Article 30 of the new Public-Contracts Code , mentions the possible cases of public contracts awarded through artificial-intelligence systems.

The provision is characterised by three aspects: what is there and is to be welcomed, what is there and has some problematic features, and finally what is missing.

First, it is worth noting how Article 30 ratifies the aforementioned principles: it is a clear declaration of intent on the desire to increase the use of new automation techniques. The transposition of the principles

[18] M.C. Cavallaro, *Imputazione e responsabilità*, 73-74, finds in reasonableness "the criterion of discernment, through which the administration can assess the outcome of the automated procedure and provide accordingly, or whether to depart from it", since "the administration's task is therefore to ascertain that the final decision, the result of an automated procedure, is not in clear contradiction with the intrinsic purpose, i.e. with the public interest, that the administration intends to pursue through the decision itself".

[19] Again, on this point, V. Brigante, *Evolving pathways of administrative decisions*, Naples, Editoriale Scientifica, 2019, 166.

formulated by case law into a regulatory provision fills Article *3-bis* of Law No 241 of 1990 with meaning, and in fact a doubt arises as to the appropriateness of the placement of this provision. In fact, it is a provision of principles, which would fit well within the general law on administrative procedure, and less so within the field of public contracts.

One criticism that can be levelled at this provision concerns the sentence "if possible'. This is an indeterminate legal concept of such latitude as to raise the question of whether the legislator meant 'legal' possibility or 'technical' possibility. On this point, all the problems resurface regarding the validity/legitimacy of an administrative measure that is entirely automated by *machine learning* algorithms, since the exercise of administrative power is lacking even in the phase of predetermination of the measure's discretionary content. Even admitting that self-learning algorithms are compatible with the network of guarantees attributed to citizens and economic operators (and on this point it is considered that there is a basic legal incompatibility), there may be several problems of 'technical feasibility' that hinder automated administrative activity: inadequately trained personnel and weak digital infrastructures (uf any) make it difficult to apply the provision.

However, does Article 30 of the public-contracts code lack anything? It lacks any reference to the issue of discretion. At this point, there are two options on the ground: either the previous caselaw rule on the irrelevance of the distinction between discretion and constraint is taken for granted; or it is confirmed that the issue is so problematic that the typification of a rigid rule that could lead to numerous procedural and procedural problems should be avoided.

The relationship between public authorities and computer algorithms is extremely complex, and the annotated case law represents another episode in a saga that is not about to end soon.

European Review of Digital Administration & Law - Erdal
2023 Erdal, Volume 4, Issue 1, pp. 313-321
ISSN 2724-5969 – ISBN 979-12-218-1128-5 – DOI 10.53136/9791221811285 26

Book Review

Giovanni Gallone: *Riserva di umanità e funzioni amministrative. Indagine sui limiti dell'automazione decisionale tra procedimento e processo,* Cedam, Milan, 2023.

1. The book by Giovanni Gallone (published by Wolters Kluwer - Cedam, Milan, 2023) offers to the attention of Italian administrative practitioners a principle, called the humanity reserve, which expresses a legal limit to the automation of the administration's decision-making processes.

The author's reflections go back a long way and have deep cultural roots.

The basic consideration is that, with the emergence of artificial intelligence, "there is no longer a sphere of exclusive human prerogative, since the intellectual sphere has also become contestable by the machine. The latter has invaded the field of intellect, competing with man on a terrain that is not that of mere physical labour. And there is a clear risk that, in perspective, the space of the person will be totally engulfed by it' (p. 16).

However, Gallone is certain that 'the protection and promotion of the human person must be the measure and end of technological development. This excludes at root that the machine can assume a significance other than that of mere instrumentum at the service of man [...]" (p. 35).

In support of this position, the author does not merely invoke the scientific authority of others. He argues how it is unacceptable that an entity devoid of conscience and incapable of making moral judgements, such as even the most refined algorithm, should prevail over man who, conversely, is the only entity endowed with conscience, 'understood as awareness of one's own and others' existence and of the consequences of one's actions' (p. 35).

Moreover, the machine has "a purely utilitarian approach to the fulfilment of collective choices", while the modern conception of justice as fairness points to "the intrinsic erroneousness of ethic hinging on the calculation of supra-individual utility as irreconcilable with the separateness of persons, i.e. with the irreducible uniqueness of the individual human beings involved in the choice".

Hence - and other outline considerations - the 'need to enucleate, in the various fields, a sphere of action that is inexorably removed from automation and reserved for humans' (p. 38). In the field of administration, artificial intelligence brings considerable advantages in terms of good performance, cost-effectiveness, overall effectiveness and efficiency and is therefore destined to find increasing use (p. 26). However, artificial intelligence also has a 'dark face' (lack of transparency, risks to the protection of personal data, software errors and cognitive biases) that can undermine the activity of the administration in relations with private individuals. This makes it imperative to reflect on the limits to its dissemination (p. 26 ff.).

2. Gallone is well aware that no provision currently in force expresses the principle of the reservation of humanity. This is why he dedicates probably the most original pages of his work to the search for the foundation of the principle, which he finds in the web of constitutional and supranational principles and in some characteristic institutions of the theoretical-dogmatic tradition of continental administrative law.

The constitutional dictate exhibits 'an absolute centrality of the human person' (p. 42), which can be seen both in the part relating to general principles and in the provisions dealing specifically with public administration. In particular, it is significant that the latter is identified not only in public offices, but above all in civil servants, to whom Art. 97(3) refers "the spheres of competence, attributions and responsibilities", and in "public employees", whom Art. 98 wants "at the exclusive service of the Nation".

The author then assigns particular importance to Article 54(2), which requires 'discipline and honour' from the 'citizens' entrusted with public functions and therefore excludes the 'possibility of entrusting the performance of administrative functions to centres of imputation that do not have a personal substratum' (p. 46); and to Article 28, considered to be 'the true cornerstone of the constitutional model of administration', which, by providing for the direct liability of officers for acts performed in violation of rights, and the liability of the administration as an extension of that of the officers, excludes the 'direct liability of officers for acts performed in violation of rights'. 28, judged to be the 'true architrave of the constitutional model of administration', which, by providing for the direct re-

sponsibility of officers for acts performed in violation of rights, and the responsibility of the administration as an extension of that of the officer, implies the logic 'of an administration that, also in terms of responsibility, is, first and foremost, made up of persons' (p. 48). The conclusion is that on the basis of the constitutional model, 'while the person is the true focus of the administration, automation is nothing more than a mere instrument' (p. 49).

Gallone believes, however, that 'the true constitutional cornerstone of the reserve of humanity' is to be found 'much deeper' (p. 52), in an intangible value that cannot be subjected to constitutional revision. In this regard, on the strength of the investigation into the cultural premises carried out in the first part of the book, the author can affirm that the reserve of humanity represents 'one of the various corollaries of the personalist principle that innervates our legal system and is enshrined in Article 2 of the Constitution' and that is linked to that of the dignity of the person. The dignity of men – observes the author – 'is measured in the relationship in which he/she is placed not only with respect to other persons (according to the guideline of equality as 'social dignity'), but also [...] with respect to what is not men and, therefore, to the machine'. Subjecting the person to fully automated decision-making is detrimental to human dignity because it subjects the person to the power of the machine. Hence, 'the protection of the dignity of the person makes [...] constitutionally necessary the intervention of men in the fulfilment of the administrative choice so as to restore the axiological hierarchy between person and machine traced by the Charter' (p. 57).

A basis for the reservation of humanity would also be found in the European Convention on Human Rights. As it is well known, Strasbourg caselaw holds that the principles laid down in Article 6 of the European Convention on Human Rights concerning the "Right to a fair trial" also apply to a portion of administrative activity, in particular its punitive activity. This, according to the A., implies that the administration "retains a human face" since "the 'court' referred to in Article 6 of the Convention (and, therefore, by virtue of the equivalence made by the Court's caselaw, also the Public Administration) is conceived, in parallel with the guarantees of a fair trial pursuant to Article 111 of the Constitution, as a 'body composed of natural persons'" (p. 63).

In conclusion, the human reserve is a principle 'immanent to the legal system' (p. 65) that 'translates, at least in its minimum meaning, into the prohibition to provide for totally automated modes of exercising authoritative capacity' (p. 66). It is a rule 'of super-primary rank' that is imposed on the legislature and the administration. And, viewed positively, it constitutes "the foundation of a specific prerogative of the citizen with respect to public power" (p. 67): the reserve of humanity as "the pillar of the nascent Italian and European digital citizenship" (p. 67).

3. We thus come to the 'theoretical-dogmatic foundation of the reserve of humanity', an aspect on which, in the opinion of the author, 'administrative scholarship has never adequately dwelt' (p. 71). Gallone observes that, according to the 'consolidated and long-standing teaching', 'the public body, like the private one, acts by means of physical persons linked to it by a specific relationship (precisely the so-called organic relationship)' and that 'from its origins the figure of the body has [...] presented a clear and well-defined anatomy according to which its ownership can only be held by a physical person' (p. 75 f.). This implies that administrative activity has always been seen as a 'human activity', insofar as it is 'referable to the public body through the officer who is a natural person and holds the quality of an organ' (p. 77); and that the main product of this activity, i.e. the administrative act, has also always been considered as a 'human' factor (p. 78): not insofar as it is an expression of the brute will of the officer, but because the imputation of the act to the body 'inevitably passes through the organ and, therefore, through the natural person who is its owner' (p. 79).

The advent of digitisation led scholarship to elaborate conceptual schemes that could do without the human basis. There was talk of the computer as a new figure of public official or of the automated administrative act as a mere fact of organisation. For Gallone, however, there have not been 'enough convincing ideas to abandon, in the legal framework of automated administrative activity, a model as dogmatically and normatively rooted and consolidated as that of organic identification' (p. 83). A model to which, according to the author, reference must necessarily be made in order "not to break the circuit of responsibility that represents one of the main factors of legitimisation of public powers" (p. 84). Article 28 of the Constitution, in fact, configures the responsibility of the body as an "extension" of the public responsibility of the official: and "conceiving a fully automated administrative activity to be imputed impersonally to the Administration as an apparatus [...] would have the effect of inhibiting this circuit of responsibil-

ity in its first segment" (p. 85).

It is not only the enduring relevance of the anthropocentric model of organic imputation that constitutes the dogmatic foundation of the administration reserve. Added to this, in the thought of the author, is the reasoned refusal to conceive of the algorithm as an administrative act. Considered in and of itself, the algorithm is, in a static sense, "the object of the preliminary administrative volition with which automation is opted for" (p. 93); and, in a dynamic sense, "an instrument of administrative action, a means in the hands of the administration that is employed between the preliminary and decisional phases". In the automation of administrative functions, therefore, at least 'two distinct moments of volition are essential': "the first, of a preliminary nature in which, upstream of the preliminary investigation, the Administration chooses (by means of an administrative or regulatory act) to use the algorithm (which, as such, forms the subject of the endoprocedural act adopted); the second, downstream of the preliminary investigation (which sees the use of the algorithm as a tool), in which the Administration makes the product of the algorithmic operation (output) its own, transposing it as the content of the conclusive procedure" (p. 98).

4. National law does not contain an organic discipline of the automation of administrative functions. However, according to Gallone, the reserve of humanity finds "a point of emergence [...] in the general law on administrative procedure, all marked, in reflection of the constitution, by the personalist principle" (p. 108). He gives the example of the person in charge of the procedure, a figure that expresses the human face of the official in the interlocution with the private individual (p. 108 f.). The sectoral disciplines confirm this approach.

Faced with a regulatory framework that is in any case laconic, case law has traced the general statute of automated administrative functions around three fundamental pillars: knowability, algorithmic non-discrimination and "non-exclusivity of the algorithmic decision". With regard to the latter, the Council of State has stated that "there must in any case exist in the decision-making process a human contribution capable of controlling, validating or refuting the automated decision" (Cons. Stato, sez. VI, 13 December 2019, no. 8474).

In this pronouncement Gallone sees the emergence of the reservation of humanity, even if the expression 'algorithmic non-exclusivity' does not give an account of the 'positive scope of the principle and how it conditions the substance of administrative action' (p. 119). The pronouncement, in any case, is considered by the A. as the starting point for further desirable insights from caselaw.

The latter should first of all take note of the constitutional and supranational basis of the principle. According to the author, in fact, it is improper to identify it, as the prevailing caselaw and scholarship do, in the right of the individual, acknowledged by Art. 22 GDPR, not to be subjected to automated decisions without human involvement and which, at the same time, produce legal effects or affect the individual in a similar way. This right - the A observes - is conferred by the provision on the natural person to whom the personal data subject to processing relates: thus, 'where the performance of automated administrative tasks does not involve the processing of personal data, the provision in question and the GDPR in general would not apply' (p. 122). And moreover, Article 22 seems to acknowledge 'a right rather than, in the negative, a prohibition and a general limit on the prerogatives of the Administration as an authority'.

Caselaw will also have to investigate the scope of the principle of the reservation of humanity, so as to arrive at the 'identification of the minimum humanity that must be guaranteed in the performance of the administrative function' (p. 118).

5. Having concluded his discourse on the foundation of the principle, Gallone opens the chapter on the 'points of emergence of the reservation of humanity in the performance of automated administrative functions' (p. 141 ff.). The premise here is that the reserve of humanity is a preceptive principle, not a merely programmatic one. In concrete terms, it translates, 'in its most elementary meaning, into an absolute (and non-derogable) prohibition of carrying out the procedure in a totally automated form' (p. 146). At a more sophisticated level it is a question of defining what the minimum of humanity in the performance of the administrative function consists of that cannot be conculcated by the administration (p. 146).

In order to proceed in this sense, Gallone considers it useful to distinguish two points of emergence of the reserve of humanity, identified in the light of what has been stated above regarding the role of the algorithm as an instrument of administrative activity.

The first point of emergence 'coincides with the moment in which the preliminary volition is expressed through which one opts for automa-

tion, defining its modalities (also through the identification of the algorithm to be employed)' (p. 148). The choice in question must necessarily fall to men because, although not decisive with respect to the content of the final decision, it has 'repercussions on the level of the modalities of the performance of the administrative function and, therefore, also on the guarantees of the interested parties' (p. 149). The preliminary volition in question may be expressed in a general and abstract form through a legislative or regulatory act, or in an administrative form by the person in charge of the procedure pursuant to Article 6(1)(b) of Law No. 241/1990, which assigns precisely to the person in charge the task of defining the modalities of the procedure. In this case it may be a specific or general administrative act, such as a call for tenders (p. 152). The author expresses a preference for the latter solution: "reasons of technical expediency push towards the standardisation of the content of administrative acts of prior volition with which automation is opted for" (p. 152). Where automation is opted for by means of an administrative act, it may be challenged cumulatively to the final measure adopted on the basis of the computational result. Where the choice to automate finds a place in a regulatory act, it will also be possible to proceed to its direct disapplication with the consequent repercussions on the fate of the final administrative decision downstream (p. 156).

The second point of emergence of the reservation of humanity coincides with the adoption of the final measure. This is the 'most delicate juncture of the entire automated administrative procedure'. Indeed, 'it is certainly possible that, once the choice has been made upstream to carry out the procedure in an automated form, the final measure is issued by the computer without any further input from a natural person. This, however, would mean subjecting the person to the authority and decision of the machine, exactly what the reservation of humanity prevents. Moreover, 'to admit that the final procedure can be packaged and issued directly by the computer [...] seems [...] incompatible with the dogmatic premises from which we started with regard to the imputation of the automated act and the nature of the algorithm', understood as a mere instrument of administrative action (p. 157). Human intervention in the adoption of the procedure is necessary, according to Gallone, even when the administrative activity is binding: even in this case 'the subjection of the person to the decision of the machine cannot be tolerated, insofar as it is detrimental to human dignity' (p. 160).

The product of the automated algorithmic operation integrates the "results of the investigation" within the meaning of Article 6(1)(e) of Law No. 241/1990. The officers endowed with decision-making power may make them their own, in which case 'the computational result is transformed into the content of the final decision', or depart from them. In both cases the officer makes 'a choice in the proper sense because it is made in the face of the practicability of an alternative in law. It is, therefore, beyond doubt that this manifestation of will, as a fully human act, retains an authentically decisional nature, with all the repercussions in terms of legal regime and protection for the addressee' (p. 166).

The risk that the officer's differing choice would nullify the advantages that can be derived from automation in terms of speed and efficiency of the administrative action is in any case contained, given that Article 6, paragraph 1, letter e) of Law No. 241/1990, which imposes an aggravated motivation for the choice to depart from the results of the preliminary investigation, places a general "duty of consistency between the outcome of the preliminary investigation and the final decision". In this regard, Gallone goes so far as to affirm that "the exceptional nature of the hypothesis suggests a taxative approach with respect to the cases that allow one to depart from the computational result, as it is not possible to admit generic motivations that are only apparent. In this sense, it would seem that they should be reduced to the extreme hypothesis of the error of calculation stricto sensu intended, to the material error committed at the time of input as well as those pertaining to the correctness of the upstream choice, at the time of the preliminary volition with which one opted for automation, of the algorithm to be employed. Another extreme hypothesis in which it is certainly permissible to depart from the computational result is that of manifest injustice, illogicality or erroneousness of the result. The latter must, however, stand out ictu oculi and impose itself with objective evidence" (p. 171).

6. The administrative decision adopted in a totally automated form for Gallone is an administrative measure that differs from its normative paradigm, and is therefore invalid. And the general schemes of the theory of invalidity must be applied. Gallone specifies that the reservation of humanity is not prescribed by a rule attributing power, understood as the rule whose sole content is to confer on the administration the 'abstract

capacity to implement an act of preceptive and authoritative content' (p. 184), but by a rule on the exercise of the power itself. It is therefore to be ruled out that the reservation of humanity constitutes a condition for the existence of power (p. 185) and that its violation causes the nullity of the measure for absolute defect of attribution pursuant to Article 21-septies, law no. 241/1990 (p. 188). More articulated is the reasoning that leads to the exclusion of nullity for lack of an essential element, in particular for lack of intention. The author considers that "in the case of the administrative measure adopted in a totally automated form, the will is not so much missing as incomplete. This is the case at least when one has opted for automation "by means of an ad hoc administrative act", since it is precisely the making of such a choice that is sufficient to acknowledge the existence "of some, albeit feeble, voluntaristic afflatus" that indirectly affects the measure. On the other hand, "a partially different discourse must, in all probability, be made with regard to the hypothesis in which automation is opted for not by means of an ad hoc administrative act, but in a general and abstract manner and in regulatory form by virtue of a provision of law or regulation that refers to a genus of procedures. In this case, in fact, there would be a complete lack of administrative volition (even if preliminary) in support of the conclusive determination adopted in a totally automated form [...] which leaves essentially open, at least with regard to this case, the problem of the subsumability of the violation of the reservation of humanity under the figure of structural nullity for lack of the essential requisite of the will" (p. 194).

Outside this hypothesis, the violation of the reservation of humanity integrates the violation of the law, cause of annulment of the measure pursuant to Article 21-octies, Law No. 241/1990. The measure is therefore liable to become unenforceable, is voidable ex officio and subject to validation pursuant to Art. 21-nonies, law no. 241/1990. The violation cannot be derubricated to "formal or procedural", possibly irrelevant for the purposes of annulment pursuant to Art. 21-octies, paragraph 2, since "human intervention in the adoption of the measure must be acknowledged as having not only procedural but also substantial and essentially organisational importance, in a manner not dissimilar to what happens for the guarantee of motivation" (p. 197).

7. Gallone in the final chapter wonders whether the principle of the reservation of humanity, as constructed by him in its assumptions and above all in its implications, is not reduced 'to little more than a dull simulacrum' (p. 201). In particular, he worries that, given the exceptional nature of the hypotheses in which the deciding body may deviate from the results of the computational investigation, human intervention may in most cases be limited to 'only an apparent supervision of the machine's work'.

But the principle of the humanity reserve also has solid constitutional foundations in the process, where it is even more pregnant as it ensures not only the humanity of the decision but also the humanity of the decision-maker (p. 218). Since the procedure and the administrative process are "contiguous and communicating planes" (p. 205) and there is a "tendency towards hybridisation of the two legal sequences" (p. 206), it can be considered that "a strong automation of the procedural phase, especially by means of artificial intelligence, is admissible and compliant with the reservation of humanity only when compensated by the guarantee of a subsequent human judicial control that is in line with the criteria of full jurisdiction" (p. 222).

That is to say, at the conclusion of the study, a parallelism is proposed between the compromise of the reservation of humanity in the proceedings and the violation of procedural guarantees in sanctioning proceedings: just as the latter can be remedied, according to the case law of the United Nations Commission on Human Rights, in the courts through the so-called review of full jurisdiction, so, according to the author, the full review by a judge 'in the flesh' allows one to consider the reservation of humanity complied with even when human intervention in the proceedings has been almost non-existent.

8. Giovanni Gallone's volume is embellished by a preface by Prof. J.B. Auby, who expresses a convinced appreciation of the research and endorsement of its results, so much so that he believes 'it is likely that, under one name or another, the principle of the "reserve of humanity" will soon be unanimously recognised as a fundamental principle of digital public law'.

Reading against this light perhaps also reveals some dissent, on aspects that are not fundamental but nevertheless important.

Auby considers the right enshrined in Article 22 of the GDPR to be 'the most important' of the rules and principles requiring the presence of the human element in public decision-making: whereas, as we have seen, Gallone expresses a strongly sceptical and minority position on this point.

Secondly, Auby considers that one can 'certainly admit that the importance attributed to the implementation of the principle [of the humanity reserve] changes according to the greater or lesser importance of the administrative decisions taken: the requirement of humanity seems particularly important when the measures have a sanctioning character, when they concern the granting of social advantages, etc.'. Presumably, a criterion of proportionality could be invoked: the requirement of humanity could be invoked in proportion to the importance of the rights and interests that the decision may involve'. Gallone's position is less elastic: the linking of the principle of the humanity reserve to the superprime value of human dignity excludes an application according to proportionality of the principle itself, and induces the Author to attribute to it the same value and scope in binding administrative activity as in discretionary activity.

9. There are two possible approaches of the jurist to the digitisation of the administration. The first consists in illustrating the phenomenon, identifying its fields of application to administrative activity, and finally considering the problems that this application poses: in a perspective that, on the whole, is to overcome them given the advantages of the advent of information technology. The second approach consists instead in starting from the legal rules on administrative activity and on the protection of the individual against power and, considering them non-negotiable, verifying to what extent and with what limits they admit the intervention of the machine.

Giovanni Gallone's approach is definitely the latter. Before him, other authors have identified the prescriptions of international, European and domestic law that place curbs on the use of machines and artificial intelligence in administrative action to protect the values of the individual. However, the interpretation of the constitutional framework proposed by Gallone is distinguished by its elegance and the stringent nature of the arguments used. Moreover, the research is nourished by an uncommon ethical tension: not concealed, indeed claimed between the lines, but always controlled, and founded on undoubtedly meditated convictions; above all, always translated into precise interpretations of regulatory provisions, especially constitutional ones, and never assumed as a direct source of rules without the need for legal intermediation.

Some perplexity may be raised with respect to some issues, but only in order to fuel the argument with the author; first of all on what remains one of the most interesting and innovative aspects of the monograph - Auby also observes this in the preface - namely the possibility of identifying the dogmatic foundation of the reserve of humanity in the theory of the organ since this, simplifying to the extreme, evokes the idea of an administration that acts through flesh and blood persons, whose acts are imputed to the organisation.

The organ theory undoubtedly has an anthropocentric basis. It starts from the assumption that legal persons are not in themselves capable of legal action, since the production of law depends on the human will. Through the organ, the legal person receives the capacity of the natural person, to the extent that he/she becomes the owner of the legal person itself, or at least acquires the capacity to impute the acts of the natural person to themselves.

However, one could object to Gallone that it is precisely the anthropocentric basis of the theory that makes its recourse questionable when the actual problem is to impute the decision of the algorithm to the entity and not to the will of a natural person. In other words, the organic theory is the instrument ordinarily (and not without exception) resorted to in order to impute the will of a natural person to the entity: once the problem of imputing the algorithm's decision to the entity, and not to the will of men, arises as a result of automation, different imputation criteria may, at least in theory, come into play. After all, what articles 28, 103 and 113 of the Constitution require (in the sense that they presuppose) is that the decision (whether men's, machine's, chance's, etc.) be imputed to the administration, so that the latter is placed in a position to answer for it, but not that the imputation take place through organic theory. But if algorithmic decision-making requires alternative imputation techniques, does it make sense to identify the organ theory as a limit to the use of automation?

Another critical point of Gallone's argument might be the follwing. If, as the A. maintains, the software does not make a choice, i.e. it does not carry out a comparison and balancing of interests, then, when the power is discretionary, the officer should be given much more leeway than G. is inclined to admit. For the A. the officer may either adhere to the results of the preliminary investigation or depart from them in the event of a computational error or manifest injustice, whereas it seems to me that, if the case is discretionary and such discretion is deemed not to have been expended by the algorithm, then the official should be able to carry out all those op-

erations of balancing and comparing interests that are properly discretionary. Which, moreover, would be an effective guarantee of the reservation of humanity in the proceedings and would remove the spectre of a merely formal human verification.

Again. If what makes the automated decision an administrative measure is the intervention of the human will, would it not be consistent to say that if such intervention is lacking and the decision is adopted in a totally automated form, then it does not constitute an administrative measure? That is, we would be in front of a non-existent measure (the non-existence of a measure), not an illegitimate measure, as the author maintains, therefore productive of legal effects and susceptible of validation.

In both these respects, the author's arguments end up weakening, perhaps excessively, the preceptive content of the principle he himself elaborated. Gallone is well aware of this and for this reason argues in the last chapter that the total absence of humanity in the proceedings can be remedied at trial, provided that the automation does not also propagate to the trial and therefore the judge remains 'human'.

That the reserve of humanity applies in the process, as much and perhaps more than in administrative activity, is certainly convincing. More doubtful is the possibility of recovering through the trial the humanity missing in the proceedings. It does not seem to me that in this regard one can apply the reasoning developed by the Court of Justice with regard to Article 6 of the European Convention on Humanity, first of all because it refers to the violation of a procedural rule, while the reservation of humanity represents a substantive guarantee, as the author of this article maintains in order to avoid the application of Article 21-octies, paragraph 2, law no. 241/1990 in the event of its violation. Moreover, the approach of the ECHR concerns, and this too the A. does not fail to point out, a well-identified portion of administrative proceedings, especially those for the imposition of administrative fines. On the contrary, if we were to consider that the violation of the reservation of humanity could be remedied by the review of the decision by a 'human' judge, we would have to assume, given that digitalisation is a pervasive and transversal phenomenon, that this possibility of remediation is also of a general nature, which in turn would really mean debasing the procedure as the place where the decision is formed, to the point of rendering it useless.

10. The doubts I have expressed on some profiles of the author's discourse do not distract from the essential point, which is that the monograph is persuasive in demonstrating that the Constitution (understood in a broad sense) prohibits a complete digitisation of administrative activity, a digitisation that would make the human face of the administration disappear.

It seems important to emphasise this research result: it is not just a prudent case law or some sporadic article of law that imposes the persistence of men as a limit to the full digitisation of administrative action, but this is a constitutional necessity, expressed by the systematic interpretation of the formal Constitution and the other above-legislative sources.

This acquisition calls into question the constitutional principle of legality, which is a constraint on the legislator, before the administration. Gallone, by denying that it is an administrative act and derubricating it as a mere instrument of administrative action, excludes that the use of the algorithm requires precise authorisation in law. On this one can probably agree. However, if the reservation of humanity is a constitutional principle, then the question that naturally arises is whether the same can and should be applied directly in the courts (or regulations), or whether rather the constitutional principle of legality of the administration, understood in a substantive sense according to the caselaw of the Constitutional Court, does not call for legislative intermediation.

Of course, that of administrative law is a history of direct application of constitutional, or institutional, principles by the special judge. It is therefore natural, and to be welcomed, that the administrative judge does not perceive the absence of an organic legislation on the reservation of administration (such cannot be considered the one contained in art. 30, par. 3, legislative decree no. 33/2023, which in any case adopts the caselaw's elaboration on algorithmic non-exclusivity) as a brake on the work of constructing a statute of digital administrative activity, which he has meritoriously begun. But this does not detract from the fact that the legislature would be fulfilling the role assigned to it by the substantive value of the principle of constitutional legality if it were to dictate such a regulation, and that only the law could ensure the organic nature of intervention that the matter requires.

Gallone's elaboration on the specific points of the emergence of the reserve of humanity in administrative action, hence on the rules that give substance to the principle (what the A. indicates

as the 'scope' of the principle) and on the consequences of their violation by the administration, is in some respects debatable, as is any original construction that aspires to preceptiveness but takes place in a normative vacuum; but it is undoubtedly reasonable (perhaps a little too rigid, but only where it refuses to calibrate the content of the reservation of humanity according to the more or less discretionary tenor of the act, an issue, moreover, pointed out by Auby in the preface), dogmatically founded, coherent and respectful of the essential and more consolidated features of the regime of the administrative act; therefore it may constitute a valuable guide for caselaw, today; and, hopefully, for the legislator, tomorrow. [Reviewed by MICHELE TRIMARCHI].

Eva Menéndez Sebastián, *From Bureaucracy to Artificial Intelligence. The Tension Between Effectiveness and Guarantees,* Cedam, Milan, 2023.

In "From bureaucracy to artificial intelligence. The tension between effectiveness and guarantees", Eva Menéndez Sebastián guides readers through a deep exploration of the evolving role of Artificial Intelligence in the dynamic framework of public governance. She provides an insightful analysis for evaluating when the use of AI can enhance public action while ensuring strict compliance with all necessary guarantees.

The book is divided into three primary chapters. In the opening chapter, the Author establishes a comprehensive framework for the analysis, discussing the transition from the traditional Weberian bureaucratic model to the evolving landscape of new public governance. This transformation is marked by the consolidation of a renewed relationship between public authorities and citizens, mainly guided by the principles of transparency, accountability, and effectiveness. The Author discusses the innovative role of good administration as a potential bridge between administrative citizenship and artificial intelligence. Algorithmic systems have the potential to enhance a more efficient allocation of resources and lower costs, thereby contributing to a better achievement of the general interest.

The second chapter is the focal contribution of the volume, aiming to provide a general analysis of the deployment of AI systems by public administrations, with a primary focus on disentangling the tension between effectiveness and guarantees. This duality is recurrent throughout the chapter, with the objective of finding a balance between risks and benefits, as well as between the compliance with due process rights and the goal of fostering innovation in implementing AI technologies. The Author begins with the following premise: the use of AI does not always necessarily lead to greater efficiency, "at least not if it is not done in the most appropriate way". This premise serves as the cornerstone guiding the entire body of the work. Public administrations need to carefully evaluate when the use of AI is functional to improve public action, and how to ensure compliance with all necessary guarantees. This volume represents a significant step forward in this direction and, by quickly discussing some critical passages of the central chapter, in the following lines I focus on explaining why.

In the first part of the second chapter, the Author delves into the deployment of AI systems in both the material and formal activities of public administration, highlighting the potential benefits of using AI to enhance decision-making processes. AI can boost three primary dimensions: the internal efficiency of the public administration, its decision-making, and the interaction between citizens and administrations. The Author stresses the imperative of aligning the functionalities of AI systems with both material and formal activities, emphasizing the salience of integrating AI with the core principles of good administration, including efficiency, transparency, accountability, and the protection of due process rights.

The Author then outlines several benefits arising from the deployment of AI technologies in public-administration activities. However, the spread of these technologies in the public sector is still facing barriers, including: (i) the lack of adequate resources; (ii) risks associated with the use of AI, such as algorithmic discrimination; (iii) insufficient access to large volumes of high-quality data; (iv) increased global competition and scattered regulation; (v) lack of trust or insufficiently understood impacts, to name just a few. On the other hand, the Author warns against the risks associated with the deployment of AI, such as the lack of adequate transparency, the difficulty to explain and motivate automatic decisions, the possibility of discrimination, or the risk of over-reliance on automation. Even beyond legal concerns, there are considerations of acceptability among citizens and public employees, as well as technical risks – although the volume does not delve into these latter aspects.

Finally, the concluding section of the second chapter underscores the importance of integrating AI systems with the core principles of good

administration while maintaining a critical perspective on the potential risks and implications of AI deployment in the public sector. The author emphasizes the need for a careful analysis and strategic planning of AI implementation, especially considering the extensive range of consequences that should be weighed before the deployment, as well as assessing its long-term implications. The author enriches the analysis with extensive reference to the legislation and the caselaw of the main European countries, as well as the European legal framework.

The volume concludes with a compelling third chapter that delves into the practical deployment of AI systems in public action. In transitioning "from theory to practice", the Author highlights three pivotal domaines where AI may be implemented successfully in the area of subvention procedures: helping the recipients or citizens, facilitating internal management, and contributing to control procedures. The provision of information to user via chatbots, the application of AI for verifying compliance with the requirements to be beneficiaries of a directly awarded subvention, and the use of blockchain technology in justification procedures, are just some examples. The final pages are dedicated to presenting a set of principles crucial for the implementation of AI in the public sector. The Author presents a comprehensive list of essential principles, such as human primacy, performance, equality, equity and non-discrimination, transparency, autonomy, environmental sustainability, proportionality, precaution, and acceptability, among others. These principles serve as a roadmap to guide the adoption, design, and implementation of AI in public action.

Two concluding observations about this volume deserve a mention. First, the Author emphasizes how important it is to raise the level of awareness of citizens and civil servants about the challenge of using AI to perform public functions. The active engagement of society and public employees, facilitated by co-creation and co-development procedures, is a pivotal factor for a successful implementation of AI in the public sector. This continued focus enriches the value and scope of the entire volume. Second, by ranging from a more general analysis to practical examples, the Author outlines a roadmap for guiding public administrations in designing, developing, and validating AI systems. By furnishing theoretical and practical foundations, the Author outlines a meta-process that every public administration should undertake to evaluate appropriateness and enhance the use of AI in the public sector. "So let's get started". [Reviewed by GIULIA G. CUSENZA].

Classificazione Decimale Dewey:

340.0285 (23.) DIRITTO. ELABORAZIONE DEI DATI

Printed in September 2023
by «The Factory S.r.l.»
00156 Roma – via Tiburtina, 912



ISSN 2724-5969

ISBN 979-12-218-1128-5

30,00 EURO