federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

PAPER – 17 NOVEMBRE 2021

Shaping the Future of Health Law: Challenges for Public Law

Research group of the Interdisciplinary Research Centre on Health Law – CeSDirSan

Report of the research presented by the research group during the International Conference ICON•S MUNDO (July 2021)

Chair: M.A. Sandulli – F. Aperio Bella
Members: F. Aperio Bella, L. Lorenzoni, N. Posteraro, M. Sinisi

New health technologies and professional's liability. How public law can prevent "remote defensive medicine"?

by Flaminia Aperio Bella
Chair in Health Law - Type B fixed-term Researcher (RTDB)
Department of Law, Roma Tre University

1. The expression "New Health Technologies" is very comprehensive and defines, in general, the provision of healthcare services through use of ICTs.

Giving some examples, it refers to the digitalization of the NHS (transformation all medical records in a digital format making the NHS paperless) and to the improvement of interoperability between IT systems in the NHS (they must 'talk to each other'). The concept involves also more complex phenomena such as Telemedicine (the provision of healthcare services at a distance through use of ICT), the use of AI for diagnostic and the use of robotic systems for direct patient care (e.g. surgery robots).

All those are eHealth tools.

2. The promotion of eHealth is an ongoing process at all levels, accelerated by the pandemic.

Institutions are facing the challenges related to ageing population, the increase in chronic diseases and limited human and financial resources. In this framework, the promotion of e-Health tools is a way to ensure health systems' sustainability. It allows innovative models of healthcare, moving away from hospital-centered systems towards integrated care, implementing personalized medicine, making it easier for citizens to have equal access to high quality care and overcoming geographical barriers.

3. Emerging digital technologies in the health sector are increasingly considered by lawmakers at all levels. Having regard to the most important EU documents on the matter, all of them emphasize the potential inadequacy in existing legal regimes in addressing new risks created by emerging digital technologies.

The first EU "eHealth action plan" of 2004 introduced the topic of e-Health as a tool to make healthcare better for European citizens and stressed that "*Another important legal issue is liability in the event of problems - such as technical malfunctions of the system, network, or provision of the service itself - that result in serious harm to a*

patient. While there are currently no specific guidelines or liability rules."[1] On 2012, the EU "eHealth Action Plan 2012-2020" maintained the same approach.[2]

Other official documents highlighted that a "*major challenge for telemedicine*" is the lack of legal clarity having regard, *inter alia*, liability.[3]

Potential inadequacy in existing legal regimes is emphasized also in other EU documents, dealing with new technologies in general. In the European Parliament resolution of 2017 about Civil Law rules on Robotics, it is stated that "*In the scenario where a robot can take autonomous decisions, the traditional rules will not suffice to give rise to legal liability for damage caused by a robot*."[4] In a more recent report on Liability for AI and other emerging digital technologies published by the European Commission, the drafters emphasized that "*A robust regulatory framework should proactively address the ethical and legal questions surrounding AI*"[5] and that the lack of legal clarity about liability might compromise the expected benefits of eHealth tools.

If the matter of eHealth entered years ago in the EU's agenda (as well as in international institution's agendas[6]), since then, we had a slow and variable uptake of digital solutions for health and care across Member States and regions.[7] Only a few Member States have clear legal frameworks.

It is not surprising bearing in mind that the Treaties let the organisation and delivery of health and social care to the responsibility of the Member States according to Art. 168 TFEU.

5. The pandemic acted as an accelerator of the spread of digital solutions for health.

The health crisis facilitated the acceptance of supply of healthcare services at a distance, because of their potential to reduce hospital congestion for patients infected with COVID-19 who do not need intensive care. Such tools were useful also for non-Covid patients (especially for chronical patients) during the suspension of "in person" treatments.

One might say that the "legal shield" for health workers at the forefront of the Covid-19 emergency contributed to such acceleration. In fact, during this pandemic, several countries, such as Italy, promulgated specific laws aiming to prevent health professionals from being targeted by legal claims.

---

[1] See Communication from the Commission on e-Health - making healthcare better for European citizens: An action plan for a European e-Health Area,(COM (2004) 356 final.

[2] See Communication from the Commission on eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, COM(2012) 736 final.

[3] See Communication from the Commission on on telemedicine for the benefit of patients, healthcare systems and society, COM/2008/0689 final.

[4] See European Parliament resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL).

[5] 2019 Report on Liability for Artificial Intelligence and other emerging digital technologies by the Expert Group on Liability and New Technologies – New Technologies Formation.

[6] The eHealth strategy of WHO World Health Organization was established on 2005

[7] "The uptake of digital solutions for health and care remained slow and varied greatly across Member States and regions" (COM(2018)233 final on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society).

It was the case both for Covid and non-Covid related treatments provided in a framework of emergency and insufficiency of available resources.

6. Having regard to the Italian legal approach to the spread of the supply of healthcare services at a distance during the pandemic, it is worth starting by saying that we use to have a very light regulatory framework compared to other European countries where systems of remote care were deeply regulated (such as France).

The only (and very generic) reference were the Guidelines of the Ministry of Health of 2014.

At the beginning of the pandemic, the use of systems of "remote healthcare" increased without express intervention of lawmakers.

In the hardest days of the "first wave" the use of Telemedicine has been informally oriented by "Interim provisions on telemedicine healthcare services during COVID-19 health emergency", enacted by the National Institute of Health (Istituto Superiore di Sanità)[8]. The document aimed at providing support for the realization of services in Telemedicine during the emergency, offering indications, identifying operational problems, and proposing solutions to proactively monitor the health conditions of both Covid and non-Covid patients.

In absence of a homogeneous legal framework, the implementation of such technologies among Regions (and even among different structures in the same Region) diverged, generating potential inequalities.

Finally, in December 2020, the Ministry of Health approved the "National Directions for the provision of Telemedicine" (Indicazioni Nazionali per l'erogazione di prestazioni di Telemedicina), an updated guidance for the use of such technologies beyond the health emergency.[9] The new Guidelines mention the "pandemic" experience as a driver of the initiative to provide for uniform and detailed guidelines at national level.

7. Beyond the pandemic, the large-scale use of eHealth tools requires addressing the challenge of liability in new technologies scenarios.

Medical malpractice in Italy crossed different phases, some scholars have spoken of "swinging malpractice"[10].

[8] Available at https://www.iss.it/documents/20126/0/Rapporto+ISS+COVID-19+n.+12+EN.pdf/14756ac0-5160-a3d8-b832-8551646ac8c7?t=1591951830300.

[9] See the agreement of 17th December 2020 of the "Conferenza permanente Stato-Regioni-Province Autonome", approving the "National Directions for the provision of Telemedicine" (Indicazioni Nazionali per l'erogazione di prestazioni di Telemedicina).

[10] C. Castronovo, Swinging malpractice. Il pendolo della responsabilità medica, in Europa e diritto privato, 2020, 3, 847 ff.

In the late '70s, thanks to the case law, we passed from physicians' immunity from liability to the «error hunting». Then, we had a growing number of litigations for malpractice, the multiplication of overlapping liability regimes and the spreading of defensive medicine.[11]

Recently, some legislative acts (2012 and 2017) took a step back, mitigating the health professional's liability and fighting defensive medicine.

New technologies bring new risks for health professionals.

Recent studies clarified that there is no room for extending some kind of legal personality to emerging digital technologies.[12] In this scenario, the principle of the "supervised autonomy of robots" implies that the human role remains crucial and that practitioners must face new sets of risks (defects or malfunctions of devices, misuse of new technologies and so on).

8. Then the question arises: how to prevent defensive medicine in new technologies scenarios?

A first solution may be to reduce liability, for instance by introducing protective legislation barring lawsuits against healthcare professionals. It may also be chosen to sanction defensive medicine, introducing specific forms of liability to reduce "defensive approach". Another path is to introduce mandatory insurance scheme[13] or even to supply the insurance system by compensation funds to protect tort victims who are entitled to compensation but whose claims cannot be satisfied. Other strategies are focused on the prevention: the training on the use of digital tools could be enhanced (bearing in mind that hospitals and structures have a duty of care to make sure health professionals receive appropriate training and exchange information about the new technologies). In fact, to give appropriate education, training and preparation for health professionals, such as doctors and care assistants, it is of the utmost importance to secure the highest degree of professional competence possible, as well as to safeguard and protect patients' health. We can also think, in the future, of new professionals clinician-informaticians. It is also possible to enact shared operating protocols to assist practitioners and to integrate models of conduct to prevent professional and organizational liability implications.

7. The choice between available strategies must be guided by the need to "resize" the role of law facing defensive medicine.

[11] Defensive medicine refers to all medical care by physicians, aimed primarily at preventing the risk of litigation (*ex multis* see R. Agarwal, A. Gupta, S. Gupta: The impact of tort reform on defensive medicine, quality of care, and physician supply: a systematic review, Health. Serv. Res. 54(4), 2019, 851 ff.,).

[12] See the already quoted 2019 Report on Liability for Artificial Intelligence, stating that "For the purposes of liability, it is not necessary to give autonomous systems a legal personality" (p. 37 ff.).

[13] Till now, the availability of liability insurance for health professionals had ambiguous effects on defensive medicine and studies demonstrated that compulsory liability insurance should not be introduced without a careful analysis of whether it is really needed (see A. Antoci, A. Fiori Maccioni, M. Galeotti, P. Russu, Defensive medicine, liability insurance and malpractice litigation in an evolutionary model, in Nonlinear Analysis: Real Word Applications 47, 2019, 414 ff., spec. 430)

It is true that streamline existing rules of liability are very important, and it is possible also to consider adaptations and amendments to existing liability rules, but we have to take into account the compliance costs related to the introduction of new rules. In addition, the diversity of emerging digital technologies and the correspondingly diverse range of risks these may pose implies that it is impossible to come up with a single solution suitable for the entire spectrum of risks. In a nutshell: one size doesn't fit all.

In conclusion, the most effective reaction to defensive medicine seems to be to focus on the restore of trust with patients. It is even more crucial having regard to the 'zero-mistake' culture of omnipotent medicine encouraged by the use of New Health Technology and the fact that ICTs enable people to become active agents in their own health journey and physicians' future is dealing with self-diagnosed cases.