A perspective on the European Health Data Space

At the time of writing this article, the European Health Data Space (EHDS) is under development. A legal definition of the primary and secondary use of health data at the supranational level is a given; however, the practice of cross-border e-health still needs to be both legally and technically reinforced. Healthcare equality and technological justice need to be observed when legislating on e-health at the national and supranational levels. Data altruism is a positive phenomenon in the secondary use of health data; nonetheless, the unethical exploitation of the health-related data of digital citizens living with a chronic illness or other ailments should be eliminated. While the extension of the European digital society to include other digital societies as a whole might happen in the far future, the early results of the already interconnected European e-health infrastructures are promising. Nevertheless, there is much to do to ensure patient safety via e-health.

Keywords: *European Health Data Space, health data protection, healthcare equality, technological justice, health data altruism, patient's right to digital self-determination*

Author Information

Máté Julesz, University of Szeged, Department of Forensic Medicine
https://orcid.org/0000-0003-0148-1857

How to cite this article:
Julesz, Máté. "A perspective on the European Health Data Space".
Információs Társadalom XXIII, no. 4 (2023): 9–21.
https://dx.doi.org/10.22503/inftars.XXIII.2023.4.1

1. Introduction

Health data constitute a national asset that may be used for various purposes. While it is important to respect patients' interests in the protection of their health data, we should not restrict the use of already existing health data for such purposes as providing healthcare services outside national borders or for secondary use. The infringement of patient's right to health data protection is not only a problem for civil and administrative law, it could also lead to criminal liability of the offender. Criminal liability is, however, the last resort of the state, and its application varies from country to country.

The administrative law on health data protection and the possible civil law consequences of a violation of the personal right to health data protection are normally a sufficient deterrent to protect health data from abuse, with no need for criminal protection.

The future European Health Data Space (EHDS) necessitates protection by law to ensure the safe operation of this e-health system across the EU. However, the development of this cross-border institution and system will likely take many years because of the prerequisite for both the legal and technical harmonization of Member States' national e-health systems.

A properly operated EHDS is a common EU goal, and all Member States' national e-health systems will join it sooner or later. National steps towards harmonization can accelerate this process. The earlier the EHDS can be put in place, the earlier the Member States' national e-health infrastructures will be integrated into this supranational e-health infrastructure. Work in this area is driven by the Member States' aim to supply their citizens with the higher level of patient safety and healthcare quality that the EHDS can provide.

2. Cybersecurity and the protection of health data

On 3 May 2022, the European Commission put forward a proposal for regulation of the EHDS to apply across the EU. National legislatures in Member States have until 2025 to respond to avoid any inconsistency between the proposed EU EHDS Regulation and their own in the same field. The EHDS Regulation will be applicable in all EU Member States from twelve months after coming into effect.

EHDS Regulation Proposal, Art. 8, declares as follows: "Where a Member State accepts the provision of telemedicine services, it shall, under the same conditions, accept the provision of the services of the same type by healthcare providers located in other Member States". The law on telemedicine has long been a battlefield for health data protection. Health data communicated through the Internet is at risk of exposure to cyberattacks. The European Network and Information Security Agency (ENISA) was thus founded by Regulation 460/2004 of the European Parliament and of the Council to strengthen trust in the digital economy, boost the resilience of the EU's infrastructure, and, ultimately, keep EU citizens digitally safe, particularly from

cyber attacks. In the period from April 2020 to June 2021, over 100 incidents were reported to ENISA from the e-health sector alone.

Both legal and ethical problems can arise from the primary and secondary use of the EHDS that is under development. For instance, in Hungary, the National eHealth Infrastructure (EESZT) was launched in 2017 with the participation of public healthcare providers and pharmacies. Under this system, from 1 January 2020, all private healthcare providers, including private dentists alike, had to join this eHealth Infrastructure and start reporting from 1 June 2020. According to Julesz (2022, 32), "Telemedicine provides an ample source of health data. There is a fine line between a legally permitted derogation from data protection and a violation of law" (see also Julesz 2020; Kovács 2022; Nyitrai 2022). This statement mainly points to the secondary use of health data, that is, the regulatory, scientific, and other important objectives that might infringe on patient privacy in a legally permitted way. In February 2021, the Finnish Innovation Fund, Sitra, started a joint action with the participation of twenty-five countries in Europe known as "Towards the European Health Data Space (TEHDAS)". The goal of TEHDAS is to offer support to EU Member States and to the European Commission in developing guidelines to foster the secondary use of health data, especially in managing and sharing data (Hendolin 2021, 16).

Health data are sensitive in most countries; however, the quality and measure of this sensitivity largely depend on the functioning of the rule of law in specific countries. Whether the GDP or wealth of a country influences the observation of health data protection at the national level is debatable, though there might be a remote correlation. The quality of the rule of law can indeed have an immediate effect on health data protection, while the level of patient safety and that of legal certainty together affect the rule of law in daily practice.

Cybersecurity is an important aspect that must be ensured, directly or partly indirectly, by the state to promote the legal rights of patients. This factor is at the root of digital data protection. As early as 1998, Marsh (1998, 180) contended that "making the medical information systems accessible by the Web raises problems of unlawful access. Therefore, another building block in society should control the Privacy and Security of the stored data". At that time, Euromed-ETS, a project financed by the EU, was engaged in telemedicine security on the Internet.

Of course, cybersecurity has other facets as well. Bányász, Tóth, and László (2022, 100) hold that "cybersecurity has become more important in many respects, as vaccine research institutions have found themselves high on the list of targets for attackers. An even more serious challenge is the vaccine-infodemic state, in which many fake news stories are spread aimed at influencing public attitudes towards certain vaccines". This is another relevant problem that has attracted the attention of today's scientists and lawmakers. The Internet is a forum for both valid and false information, and is only partly regulated by legislative measures. Ethical behaviour among Internet users is simultaneously needed to provide patients/citizens with trustworthy information on healthcare products and to keep patient health data safe and secure.

Krzanowski and Polak (2022, 44) contend that the Internet as an epistemic agent endeavours to rid us of our individual worldviews and substitute them for those that favour its own epistemic agency positions and objectives (see also Héder et al. 2022). This assertion is obviously true; however, there are many other factors that impact individuals' opinions on their respective national healthcare systems and healthcare in general. The universal values expressed by international legal documents highlight the basic principles that regulate the doctor–patient relationship. In fact, protecting patient health data is one of the most important tasks for healthcare providers today. The Treaty on the Functioning of the European Union, Art. 16, para. 2, declares that the European Parliament and the Council shall "lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices, and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data".

3. The European Health Union and data ownership

Sandra Gallina, head of the European Commission's Directorate General for Health and Food Safety, argues that "The EU4Health programme will add €5.3 billion in health promotion, diagnosis and treatment, and care to help countries boost their health systems, strengthen their healthcare workforce, invest in trainings and advance their digital transformation" (Gallina 2023, 2). Gallina underlines the importance of the creation of a well-functioning European Health Union. I hold the same position. The EU4Health programme and similar initiatives provide financial aid to the construction of this long-awaited legal institution. Indeed, the practice of health law is strongly linked to health data, and, without safe health data processing, European health law would remain a lame duck.

The EHDS, the creation of which is envisaged at the moment of writing this article, would be a domain-specific common European data space. It would serve to protect individuals' health data and provide them with the opportunity to control their data. It would also help scholars, statisticians, health policymakers, and legislators retrieve the data necessary for the *commoda publica*. This last possibility (the secondary use of health data) requires a fair balance between patients' individual interests and the political, civil, economic, social, and cultural development of society as a whole. MedTech Europe was founded in 2012 to promote the medical technology industry. Horgan et al. (2022, 10) point out that "MedTech Europe highlighted the need for a health data ecosystem that fosters trust and protects individuals' rights while unlocking the great potential of health data".

Article 12, para. 4, of the European Commission's proposed EHDS regulation declares the following: "The Commission shall, by means of implementing acts, adopt the necessary measures for the technical development of MyHealth@EU." Via MyHealth@EU, the citizens of an EU Member State can safely communicate their health data in the language of another Member State. Healthcare documentation is thus available not only in the patient's language, but also in the language of physicians

practising in other Member States. The data safety ensured by the GDPR (General Data Protection Regulation) needs to be respected when putting the free movement of health data into practice. I would also wish to emphasize the role of electronic health data in the administrative health law of national legal systems. This is an opportunity that is also found in the institution of the EHDS. In my opinion, it is always best to build on already existing infrastructure and legal institutions. In this respect, MyHealth@EU represents common ground in the EU. The existing technologies furnish e-health with immeasurable experience that newly set-up technologies could only make possible in the long run.

According to 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, it is already possible, for example, to obtain medicine in an EU Member State that has been prescribed in another EU Member State. Unfortunately, this has not yet been applied in all Member States. According to a recent survey, "most responses highlighted that most EU countries have not yet fully implemented open infrastructures for data sharing" (Hussein et al. 2023, 4). However, if medicine is e-prescribed in Hungary, it is obtainable in a pharmacy in Poland. In addition, in Croatia, the Electronic Health Record contains information on a patient's condition (such as an allergy) in Czech, English, Spanish, and other languages, which might be life-saving for that EU citizen in an emergency situation where the attending physician needs instant knowledge of the patient's history. Stellmach et al. (2022, 135) maintain that "The recommendations set out in the EIT [European Institute of Innovation & Technology] would need to be addressed by the European Commission in the future so that developers and providers of EHR [Electronic Health Record] systems, products and services can be given a catalogue of approved international interoperability standards for semantics and syntax that need to be adopted". The already existing International Patient Summary could be one of those standards. These patient summaries only contain the essential health information linked to a patient, thus making it possible to treat the patient abroad when necessary. However, this information might not be sufficient to initiate medical malpractice litigation. More detailed healthcare documentation would be required for that purpose. On the one hand, the EHDS certainly would not provide the patient's lawyer with sufficient evidence to use against the healthcare provider. On the other hand, the provider would not be able to build their defence merely on health information retrieved from the EHDS. The electronic healthcare documentation necessary for litigation should be sought in the national e-health systems of the Member States, such as the National eHealth Infrastructure (EESZT) in Hungary.

Ursitti (2022, 126) argues that, "In the pre-industrial era, the gap between producing and imagining was imperceptible, worthless and harmless; today, that is no longer the case". I share this opinion. Directive 2011/24/EU, Art. 14, declares that "The Union shall support and facilitate cooperation and the exchange of information among Member States working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States". However, it could be postulated that providing patients with the right to the control of and access to their e-health data has partly remained a dream in EU Member States because of its voluntariness.

The values represented by the supranational EU law mostly derive from universal values. Nevertheless, there might be some conflicts between laws at the national and EU levels. Generally, however, Member States' legislation tends to strictly abide by EU law. In my opinion, with regard to personal rights to health and health data protection, there is no inconsistency between the supranational and national legislation. Hussein et al. (2023, 4) arrived at the following result: "Concerning data ownership, most responses from the EU countries indicated that citizens own their health data. This result could be a direct reflection of the wide implementation of the GDPR across Europe". Hussein et al. (2023, 4) also concluded that "the results of the trustworthiness of health data are relatively high".

4. Healthcare equality and technological justice

Genovese et al. (2022, 369) maintain that "None of the big health data transitions can happen without society's trust in the process". I think that, among other relevant aspects, the principle of healthcare equality also applies. The same level of healthcare should be provided for all patients, regardless of their real chance of gaining digital access to their health data. Patients should be assured that they can receive a standard level of healthcare within the EU independently of their ability to digitally control and manage their health data. Yet today, the same level of healthcare cannot be found in all EU Member States.

In addition to these remarks, there are also other noticeable comments on the EHDS in the professional literature. For example, van Kessel et al. (2022, 1) contend that "the EHDS might unintentionally disadvantage certain populations, including older people, refugees, those on low incomes, those living with chronic conditions, and some ethnic minority communities". All these groups have special features that preclude them from normal life. Positive discrimination is thus a legal and ethical must to attain social justice and technological justice. EU court practice has already acknowledged the legality of similar positive discrimination, for example, in the case of job applications. Indeed, positive discrimination is rooted in the fabric of European law and values, and needs to be maintained and even further developed. Furthermore, the EU Member States should constitutionalize the institution of positive discrimination in legal matters as well as in the functioning of the state, society, and economy as a whole. There is still a constitutional gap in this area in some European legal systems, which reflects ethical defects that need to be overcome by regulatory measures. Digitally disadvantaged minorities, whether ethnic or other kinds, should be integrated into the digital society so as to finally establish supranational technological justice. This would be the first step towards the creation of a global, or at least a regional, digital society without the need for political globalization.

In its 2022 EHDS proposal, the Commission alluded to the subsidiarity of the regulation when referring to the present-day deficiency of health data portability and to the lack of interoperability of national, regional and local e-health information systems. These deficiencies increase healthcare inequalities and should be

remedied by EU law. The existing technological injustice hampers social cohesion. While the EU's legislative efforts in this area are clear, it is too early to predict the possible outcomes of putting the EHDS into action.

Butcher (2009, 57) argues that "by maximizing the liberties (freedom to use, freedom to distribute, freedom to modify and so on) associated with certain computer software, an incentives-rich and stable environment can be established in ICT [Information and Communication Technology] that will foster development of the information economy among the information poor." I agree. However, the "information oligarchy", also noted by Butcher (2009, 59), might pose a real threat to society and the economy. I think we should have earlier prevented the technological, legal and economic predominance of a relatively small number of information-wealthy social actors. Now, it seems too late. Legislators' hands are tied by the digital practice in effect today. There is thus little space remaining for the state to place the information society, including e-health, not only on a legal footing, but also on an ethical one. All that might lead to deficiencies in technological justice, entailing healthcare inequalities as well.

Nutbeam and Lloyd (2021, 162) differentiate between functional, interactive and critical health literacy; whereby, functional health literacy refers to knowing how to use the health system; interactive health literacy encompasses the application of health information to the circumstances, including interactions with other people, to make decisions; and critical health literacy is the ability to critically analyse health information taken from various sources, resulting in an in-depth understanding of the social, environmental and economic determinants of health. I think all three types of health literacy are necessary for healthcare equality. I hold that interactive and critical health literacy cannot work without functional health literacy. In fact, the EHDS can only function well in societies where digital citizens recognize the relevance of this triad.

I side with Csótó in accentuating that, although economic poverty often goes hand in hand with information poverty, there is not necessarily a causal connection between the two; indeed, a better-off citizen may also be information poor (Csótó 2017, 26). I think, nowadays, this argument is highly significant because our information society tends to exclude the information poor. This tendency needs to be overcome by promoting social justice – and not only legislatively. I am convinced that patients whose e-health literacy is not in line with that of the majority patient population might suffer healthcare inequalities in the long run. There are many who do not use digital devices. Rab and Török (2022, 95) found that in Hungary, for example, 9.2% of the adult population has no smartphone, smart TV, laptop, PC or smart watch and is therefore excluded from the information society and thus e-health. I suppose the imminence of the EHDS can accelerate the digitalization of the European social strata now lagging behind. However, we should concentrate not on the states themselves, but rather on the disadvantaged groups within the European societies. Help ought to be given to those excluded from technological justice and facing healthcare inequality. While the principle of equality is rooted in ethics, its realization is largely dependent on social capital.

5. Health data altruism

In its 2022 regulatory proposal, the European Commission considered the EHDS as a cornerstone of the European Health Union. The Commission stressed the difficulties that EU citizens face because of insufficiencies in the implementation of the GDPR in Member States. The Commission also referred to the COVID-19 pandemic, which has recently highlighted the necessity for a safe and secure cross-border access to health data.

While it is true that the COVID-19 pandemic refined the aims of the EHDS, the basic values and legal norms tied to the EHDS have not changed. Privacy and health data protection remain primary, and legal exceptions are intended to promote the greater good, that is, public health and scientific research. Undoubtedly though, community health gained in importance during the pandemic. In my opinion, the EHDS should also be a tool in the service of promoting community health. Healthcare workers and local volunteers should be granted authorization to retrieve health data when necessary for the maintenance of the community health. This is a sensitive question because a great many individual patients certainly would not agree to this kind of disclosure of their health data. Therefore, there should be adequately elaborated checks and balances to extend the scope of the EHDS to include community health.

Health data altruism is the disclosing of patients' health data voluntarily and free of charge. With the introduction of the EHDS, the EU also aims to stress the control of data altruism. A rulebook should be implemented to determine the necessary criteria for data altruism tied to health data. It may be necessary, for example, to permit authorized persons to gain access to health data purely to promote their work in the service of the public. However, I think data altruism may lead to possible abuse of data, which would be counterproductive both for patients and society. In a top-down way, a rigorous rulebook would help determine the framework for data altruism as concerns the EHDS. The Data Governance Act will introduce the institution of data altruism in the EU from September 2023. Bottom-up data altruism remains an ethical option for individuals. Therefore, these individuals should enjoy some sort of legal protection by the EU and the Member States. Certainly, there will be legal disputes on how it is introduced, and the acceptable measure and quality of data altruism will likely arise from those disputes at the national and supranational levels. Shabani (2022, 1359) contends that "Newly proposed data altruism consent … integrates the element of multiple secondary uses of data. The upcoming EHDS regulation should clarify how these consent models will interplay in the context of secondary uses of data in the framework of the EHDS".

As a result of a global study involving 880 participants, Gefen et al. (2020, 552) concluded that "Our findings show that 99% of people were willing to contribute their data in exchange for monetary compensation and an analysis of their data, while 53% were willing to pay to have their data analyzed". As to the EHDS, I think payments to data owners could be permitted for the secondary use of their health data. I believe this option would not run counter to the EU's basic rights and values.

I thus admit that a price could be put on health data. This price would be compensation for patients abandoning their right to privacy. Naturally, however, personal rights are of an absolute character, so everyone must observe them. Indeed, Art. 16, para. 1, of the Treaty on the Functioning of the European Union declares that "everyone has the right to the protection of personal data concerning them". Nonetheless, this does not exclude data owners' right to accept payment in exchange for the commercial use of their data. In my opinion, payment would only be acceptable for a commercial secondary use of health data. All other secondary uses should be either based on data altruism or legal permission. Ethically, data altruism precedes the commercialization of health data. In today's legal, social and economic environments, the use of health data is too important to renounce for financial reasons. There is a fine line between legally and ethically acceptable data altruism and individuals monetizing their health data. In the EU, the personal data economy is increasingly fuelling present-day public governance.

I believe that the use of health data cannot be restricted to healthcare facilities and pharmacies. National e-health infrastructures are linked to national health administration systems, and individuals' health data are ultimately also used in administrative and judicial procedures. In my opinion, such use of health data should not be onerous, and data owners should not be allowed to request payment. However, digital citizens may at times be unaware of the fact that software processes their health-related data, which has been collected from web browsers. This kind of health data use seems to be controversial both economically and legally. I think those who draw profit from it should either pay for the health information under civil law or forsake this practice. The effective administrative or criminal sanctioning of health data abuses is a public law response to the issue. We should put an end to the unethical exploitation of digital citizens living with health problems by all means.

6. The patient's right to digital self-determination

Cingolani et al. (2023, 5) argue that "the implementation of AI [artificial intelligence] must be accompanied by careful reflection on the part of the legislator to ensure that the rights of citizens and patients are truly protected. For example, there is the question of consent to the processing of personal health data by artificial intelligence systems" (see also Héder 2021). Normally, governments and firms make use of artificial intelligence in processing big data. As a consequence, some countries have taken measures to account for this. In Germany, for example, a "computer fundamental right" was defined by the Federal Constitutional Court on 27 February 2008 to prevent any abuse of information systems (Hooghiemstra 2019, 172).

According to GDPR, Art. 9, the processing of health data is prohibited as a general rule. Nevertheless, it is permitted when necessary for such areas as medical diagnosis and treatment or for protection against serious cross-border threats to health. Article 9, para. 4, declares *expressis verbis* that "Member States may maintain or

introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health". This rule defers to national legislatures to adopt stricter rules when necessary. If it is consistent with this right, a Member State's national legislation cannot be successfully challenged before the EU Court of Justice. Usually, a legally protected interest may enjoy more rigorous protection than required by an EU directive. A number of EU regulations also contain a similar extension of the protection by national law.

Patients' right to self-determination is a basic right that should be observed not only by national e-health infrastructures, but also by the EHDS. Access to patients' health data on areas such as addictive and psychiatric diseases, AIDS and sexually transmitted diseases, ought to be restricted *a priori*. The sensitivity of health data varies, but unless the patient explicitly grants permission to disclose such data, they should not be accessible. The EHDS must not be permitted to lead to data abuse. Overall, patients ought to be allowed to limit access to any of their health data. These data should only be available to the attending physician without restriction in the case of an emergency to save the patient's or another natural person's life and health. In addition, the person, the date and the reason for access should be indicated, so that, later, the legality of such access may be checked.

Patients should be entitled to restrict access to their healthcare documents and other health data in a way that only the treating doctor and the primary care physician can see them. Pharmacists' access to health data could also be limited to e-prescription data.

It is important to protect health data; however, patients exercising their right to restrict access to their health data have to bear some responsibility too. A lack of information might mislead the healthcare provider. The patient's right to self-determination is constitutionalized in most democratic states under the rule of law. In healthcare, from a legal aspect, digital self-determination essentially differs from the old perception of self-determination. Furthermore, e-health may result in a legally more transparent medical practice because of the rigorous application of its clear-cut rules. I wish to stress that the exercise of a citizen's right to self-determination must not be detrimental to other citizens' right to life and health. In healthcare, the duty of professional secrecy may be overriden in such a situation. This is more than an ethical question: it is the community's legal right to self-defence that is recognised by the social actors as well as by the judiciary.

Patient autonomy has been the focus of a great many discussions on healthcare. I hold that patient autonomy can strengthen a healthcare provider's sense of security because the patient thus takes over ethical responsibility from the provider to a certain extent. Indeed, e-health may be instrumental in the realisation of patient autonomy. I believe that, considering the pros and cons of e-health, the pros prevail. The patient's right to self-determination is at the core of healthcare practice, while the patient's consent is a precondition for healthcare services, including making a diagnosis, medical treatment and any other matter entailing health data processing.

7. Conclusion

The EHDS is an EU e-health infrastructure project currently under development. Besides the primary use of health data, its secondary use is also of great importance. Health data constitute a national asset, which could be expanded supranationally. Health data altruism is not only an ethical topic. In my opinion, digital citizens' health data should not be exposed to commercial data harvesting without informed consent and monetary compensation. However, the secondary use of health data for scientific purposes or for the making of health policy or in legal procedures needs to remain free of charge.

National e-health infrastructures should be connected to the EHDS to advance telemedicine, patient safety and the secondary use of health data at the supranational level. Yet while some EU Member States' national e-health infrastructures are already interlinked, there is still a long road ahead to link them all. For instance, medicine e-prescribed in Hungary may be obtained in pharmacies in Poland.

Certainly, cybersecurity is a key issue in health data protection. Further, patients' right to digital self-determination may serve to provide legal protection for health data. Indeed, I believe achieving healthcare equality and technological justice should be fundamental social aims of the EU because an adequately operated supranational e-health infrastructure impacts not only the quality of cross-border healthcare, but also the functioning of European societies. Importantly, widespread e-health literacy – mainly though not only – in the eastern part of the EU is a precondition for putting the EHDS into effect. As a consequence of digital globalisation, technological justice and healthcare equality are strongly interrelated. In addition to legislative measures, bottom-up social effects may also improve the quality of e-health in the EU. Connecting the forthcoming EHDS to the e-health infrastructures in other (groups of) democratic countries (such as that of the US) safely and securely could give rise to a global digital society without the need for political globalisation.

References

Bányász, Péter, András Tóth, and Gábor László. "A sentiment analysis of the civic attitude in connection with the coronavirus vaccines." *Információs Társadalom* 22, no. 1 (2022): 99–125. https://dx.doi.org/10.22503/inftars.XXII.2022.1.6

Butcher, Matthew P. "At the foundations of information justice." *Ethics and Information Technology* 11, no. 1 (2009): 57–69. https://doi.org/10.1007/s10676-009-9181-2

Cingolani, Mariano, Roberto Scendoni, Piergiorgio Fedeli, and Fabio Cembrani. "Artificial intelligence and digital medicine for integrated home care services in Italy: Opportunities and limits." *Frontiers in Public Health* 10 (2023): Article Number 1095001. https://doi.org/10.3389/fpubh.2022.1095001

Csótó, Mihály. “Are the poorest the information poor? The various forms of information poverty.” *Információs Társadalom* 17, no. 2 (2017): 8–29. https://dx.doi.org/10.22503/inftars.XVII.2017.2.1

Gallina, Sandra. “Preparing Europe for future health threats and crises: the European Health Union.” *Eurosurveillance* 28, no. 5 (2023): Article Number 2300066. https://www.eurosurveillance.org/content/10.2807/1560-7917.ES.2023.28.5.2300066

Gefen, Gilie, Omer Ben-Porat, Moshe Tennenholtz, and Elad Yom-Tov. “Privacy, Altruism, and Experience: Estimating the Perceived Value of Internet Data for Medical Uses.” In *WWW ‘20: Companion Proceedings of the Web Conference 2020*, 552–556. Taipei, Taiwan: WWW: International World Wide Web Conference, 2020. https://dx.doi.org/10.1145/3366424.3383414

Genovese, Stefano, Rafael Bengoa, John Bowis, Mary Harney, Bastian Hauck, Michel Pinget, Mike Leers, Tarja Stenvall, and Nick Guldemond. “The European Health Data Space: a step towards digital and integrated care systems.” *Journal of Integrated Care* 30, no. 4 (2022): 363–372. https://doi.org/10.1108/JICA-11-2021-0059

Héder, Mihály. “AI and the resurrection of Technological Determinism.” *Információs Társadalom* 21, no. 2 (2021): 119–130. https://dx.doi.org/10.22503/inftars.XXI.2021.2.8

Héder, Mihály, Ernő Rigó, Dorottya Medgyesi, Róbert Lovas, Szabolcs Tenczer, Ferenc Török, Attila Farkas, Márk Emődi, József Kadlecsik, György Mező, Ádám Pintér, and Péter Kacsuk. “The Past, Present and Future of the ELKH Cloud.” *Információs Társadalom* 22, no. 2 (2022): 128–137. https://dx.doi.org/10.22503/inftars.XXII.2022.2.8

Hendolin, Minna. “Towards the European Health Data Space: from diversity to a common framework.” *Eurohealth* 27, no. 2 (2021): 15–17. https://apps.who.int/iris/bitstream/handle/10665/352268/Eurohealth-27-2-15-17-eng.pdf

Hooghiemstra, Theo. “Informational Self-Determination, Digital Health and New Features of Data Protection.” *European Data Protection Law Review* 5, no. 2 (2019): 160–174. https://doi.org/10.21552/edpl/2019/2/6

Horgan, Denis, Marian Hajduch, Marilena Vrana, Jeannette Soderberg, Nigel Hughes, Muhammad Imran Omar, Jonathan A. Lal, Marta Kozaric, Fidelia Cascini, Verena Thaler, Oriol Solà-Morales, Mário Romão, Frédéric Destrebecq, and Edith Sky Gross. “European Health Data Space – An Opportunity Now to Grasp the Future of Data-Driven Healthcare.” *Healthcare* 10, no. 9 (2022): Article Number 1629. https://doi.org/10.3390/healthcare10091629

Hussein, Rada, Lucas Scherdel, Frederic Nicolet, and Fernando Martin-Sanchez. “Towards the European Health Data Space (EHDS) ecosystem: A survey research on future health data scenarios.” *International Journal of Medical Informatics* 170 (2023): Article Number 104949. https://doi.org/10.1016/j.ijmedinf.2022.104949

Julesz, Máté. “Health equity and health data protection related to telemedicine amid the COVID-19 pandemic.” *Információs Társadalom* 22, no. 2 (2022): 27–38. https://dx.doi.org/10.22503/inftars.XXII.2022.2.2

Julesz, Máté. “Telemedicine and COVID–19 pandemic.” *Információs Társadalom* 20, no. 3 (2020): 27–38. https://dx.doi.org/10.22503/inftars.XX.2020.3.2

Kovács, Gábor. "Liability issues of the telemedicine service." *Információs Társadalom* 22, no. 3 (2022): 61–74. https://dx.doi.org/10.22503/inftars.XXII.2022.3.4

Krzanowski, Roman, and Pawel Polak. "The Internet as an Epistemic Agent (EA)." *Információs Társadalom* 22, no. 2 (2022): 39–56. https://dx.doi.org/10.22503/inftars.XXII.2022.2.3

Marsh, Andy. "The Creation of a global telemedical information society." *International Journal of Medical Informatics* 49, no. 2 (1998): 173–193. https://doi.org/10.1016/S1386-5056(98)00039-2

Nutbeam, Don, and Jane E. Lloyd. "Understanding and Responding to Health Literacy as a Social Determinant of Health." *Annual Review of Public Health* 42 (2021): 159–173. https://doi.org/10.1146/annurev-publhealth-090419-102529

Nyitrai, Endre. "The importance of national data assets in the work of law enforcement agencies." *Információs Társadalom* 22, no. 1 (2022): 67–80. https://dx.doi.org/10.22503/inftars.XXII.2022.1.4

Rab, Árpád, and Bernát Török. "The technological environment of e-health in Hungarian society." *Információs Társadalom* 22, no. 3 (2022): 93–99. https://dx.doi.org/10.22503/inftars.XXII.2022.3.6

Shabani, Mahsa. "Will the European Health Data Space change data sharing rules?" *Science* 375, no. 6587 (2022): 1357–1359. https://doi.org/10.1126/science.abn4874

Stellmach, Caroline, Michael R. Muzoora, and Sylvia Thun. "Digitalization of Health Data: Interoperability of the Proposed European Health Data Space." *Studies in Health Technology and Informatics* 298 (2022): 132–136. https://doi.org/10.3233/SHTI220922

Ursitti, Filippo. "The techne as producer of outdated humans." *Információs Társadalom* 22, no. 2 (2022): 117–127. https://dx.doi.org/10.22503/inftars.XXII.2022.2.7

van Kessel, Robin, Brian Li Han Wong, Rebecca Forman, Jonila Gabrani, and Elias Mossialos. "The European Health Data Space fails to bridge digital divides." *British Medical Journal* 378 (2022): Article Number e071913. http://dx.doi.org/10.1136/bmj-2022-071913