CROSS-BORDER HEALTH DATA FROM LEGISLATION TO IMPLEMENTATION A CRITICAL DISCURSIVE APPROACH TO COVID-19 RESPONSES[1]

Maria Cristina Paganoni,
University of Milan, Italy,
https://orcid.org/0000-0002-5828-8604

Abstract. With a focus on health datafication in the European Union, this article sets out to investigate a few highlights from the EU's pronouncements on issues of public health and technology, through the tools of Critical Discourse Studies. As an unprecedented public health crisis, the COVID-19 pandemic has revealed that, when it comes to healthcare, EU countries are disconnected from one another. In fact, health datafication is misaligned between Member States and even within national health systems themselves. However, the tech solutionist position that strives for full interoperability of systems in public health (as for contact tracing apps) often disregards the ethical, legal and social issues related to the use of technology itself, i. e. data protection, impact and trust. The aim of the analysis is to illustrate the role of the linguistic and discursive framing of the values and priorities that inform the debate about pandemic response management, to which millions of EU citizens have been exposed in the last two years.

Keywords: contact tracing, Critical Discourse Studies, ethics, health datafication, interoperability, linguistic framing

INTRODUCTION

This paper intends to address the issue of health datafication and data sharing across European borders, scrutinising its several dimensions by means of a critical approach that addresses socio-technical innovations and their uptake in the European Union. The modernisation and digitalisation of health systems and infrastructure are one of the four strategic goals of EU policies and actions in public health. Together with protection against serious cross-border threats to health, access to healthcare and the sharing of health data are overt priorities in the EU agenda.

The notion of interoperability should be introduced at this point as the ability of disparate computer systems or software to exchange data in an efficient and meaningful way. Interoperability in healthcare refers to timely and secure access, and integration and use of electronic health data so that it can be used to optimise health outcomes for individuals and populations. Despite indisputable benefits, however, «interoperability has been identified as one of the greatest challenges in healthcare IT» (ReEIF, 2015). It should be pointed out that interoperability is not just semantic and technical but also legal, which explains why these issues are also debated within the realm of legal communication.

[1] This article originates from the 4EU+ University Alliance research project "Transnational Legal Communication on COVID-19: From Legislative to Popular Discourse", under Flagship 2 "Europe in a Changing World: Understanding Societies, Economies, Cultures and Languages", coordinated by prof. Joanna Osiejewicz of the University of Warsaw.

In 2012, with this objective in mind, the European Commission (EC) financed an eHealth Interoperability Framework that was then refined in 2018, highlighting the need to improve the standardisation of eHealth solutions in support to health system reforms.

The eHealth Digital Service Infrastructure (eHDSI) is an infrastructure ensuring the continuity of care for European citizens while they are travelling abroad in the EU. This gives EU countries the possibility to exchange health data in a *secure, efficient and interoperable* way (European Commission website, *emphasis added*).

Interoperable medical data include Electronic Health Records (EHRs) such as (a) Patient Summary; (b) ePrescription/eDispensation; (c) Laboratory results; (d) Medical imaging and reports; (e) Hospital discharge reports (EC, 2019). In 2021 a new legislative proposal to create a European health data space was advanced to facilitate the exchange of health data across Europe, while ensuring privacy over data. At present, the sharing of health data across borders is made feasible by EHR optimisation, the implementation of digital tools and the uptake of apps.

The focus on health data sharing, which is a fundamental part of the digital transformation in healthcare, is seen against the background of the COVID-19 pandemic and the responses implemented by Member States, nationally and internationally. Pandemic surveillance has highlighted the importance of full compliance with data protection levels within the framework of the GDPR (Paganoni, 2020) and the objectives of the 2019 Commission Recommendation (Bincoletto, 2020). That is to say that technologies developed to control the spread of the pandemic should never infringe upon user privacy. While EU digital COVID certificates have made travelling possible again, contact tracing apps have not met expectations so far.

MATERIALS AND METHODS

Besides Regulation (EU) 2016/679 (hereinafter: GDPR), which mandates the rules for processing personal data for all Member States, the data set under analysis is composed of seven official documents at EU level, dealing with healthcare provision and characterised by a noticeable degree of interdiscursivity between different domains (legal, institutional, medical, technical). Moreover, the span of a decade (2011–2021) encompassed in this overview helps to set in context the development of the digital transition in healthcare.

The data set includes:

- Directive 2011/24/EU on the application of patients' rights in cross-border healthcare. It ensures the continuity of care for European citizens across borders, giving Member States the possibility to exchange health data in a secure, efficient and interoperable way. It aims to guarantee patient mobility and the free provision of healthcare services (9 March 2011);
- Commission Recommendation (EU) 2019/243 on a European Electronic Health Record exchange format (6 February 2019);
- Commission Recommendation (EU) 2020/518 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (8 April 2020);
- Communication from the Commission C/2020/2523: Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection (17 April 2020);

- Council Conclusions on COVID-19 Lessons Learned in Health 2020/C450/01 (28 December 2020);
- *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR* (11 February 2021);
- eHealth Network Guidelines on Interoperability of Health Certificates (12 March 2021).

The textual materials are scrutinised through the lens of Critical Discourse Studies (Tannen, Hamilton & Schriffin, 2015; Xenitidou & Gunnarsdóttir, 2019), identifying main concepts and keywords and paying specific attention to the linguistic and discursive framing of health datafication before and after the pandemic, with the GDPR always in the background. The analysis reflects on how health data flows across borders and their interoperability are discursively framed between opportunities yet to be fully exploited and obstacles that are both technical and legal.

RESULTS AND DISCUSSION

Directive 2011/24/EU considers «the health systems in the Union» to be «a central component of the Union's high levels of social protection» and «part of the wider framework of services of general interest» (Recital 3). Data are framed between two rights, freedom of movement and privacy. «Personal data should be able to flow from one Member State to another, but at the same time the fundamental rights of the individuals should be safeguarded» (Recital 25). Next, the Directive introduces the concept of innovation in medicine and takes «new health technologies to ensure safe, high- quality and efficient healthcare» (Recital 58). Article 12 includes *epidemiological surveillance* among its objectives. Lastly, Article 14 of the Directive sets up the eHealth Network, «a voluntary network connecting national authorities responsible for eHealth designated by the Member States». The goal is that of «delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare» (Article 14.2.a).

When cross- border scenarios are foreseen, the interoperability of applications and of EHR systems is weighed against public health concerns. A few years after Directive 2011/24/EU, when benefits as well as challenges of big data in healthcare have become more evident, these issues are addressed in the GDPR from a legal, organisational and technical perspective, when discussing data portability. In sum, the interoperability context does not exempt data controllers from implementing organisational and technical measures for ensuring data protection (Bincoletto, 2021).

Nevertheless, the GDPR mentions «health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health» as grounds to derogate from data protection. «Such a derogation may be made for health purposes, including public health and the management of health-care services, the prevention or control of communicable diseases and other serious threats to health» (Recital 52). Without a doubt, measures to fight the COVID-19 pandemic can be included here.

Developing from the GDPR and the focus placed on the rights of *data subjects*, Recommendation 2019/243 addresses *citizens* first, *healthcare providers* and then *patients*, foreseeing an increase in healthcare needs and spending «as a result of population ageing, rising prevalence of chronic conditions and a rise in demand for long-term care» (Recital 4). It argues that «the highest possible standards for security and data protection are central to developing and exchanging electronic health records» (Recital 12), emphasising the right to securely access personal data (we count four occurrences of *secure access* and six of *securely*) and protect them from *data breaches*. However, it constructs patients as a homogenous group, conversant with digital technologies, which is not often the case with elderly people, the disabled or simply European citizens that happen to be «(dis)connected in a hyperconnected world» (Xenitidou & Gunnarsdóttir, 2019, p. 302) and may be unfit to engage actively in their healthcare and wellness management.

Quite understandably, Recommendation 2019/243 sets out a framework for the development of a European electronic health record exchange format, «minimising the risk of possible tampering and misuse» (Recital 13) and building strong *cybersecurity*. Digital technologies such as health apps and wearable devices are promoted, while more interoperable electronic health systems may «give citizens greater control over their health data» (Recital 6), at the same time reducing «the costs associated with healthcare for individuals and households» (Recital 5). While «new technologies for health should support citizens to become active agents of their own health journey» (Recital 9), «the lack of interoperability with regard to electronic health records leads to fragmentation and a lower quality of cross-border healthcare provision» (Recital 11). Agency in a patient's lifestyle is thus emphasised, while incompatibility and fragmentation of electronic health records are denounced. Lastly, «new technologies, such as big data analytics and artificial intelligence can support the search for new scientific discoveries» (Recital 18).

From the start, Recommendation 2020/518 frames the COVID-19 pandemic as «a public health crisis» and «an unprecedented challenge to [*the EU's*] health care systems, way of life, economic stability and values» (Recital 1). It outlines a European approach to the pandemic and proposes «a number of steps and measures for developing a common approach to the use of mobile applications and mobile data», stressing that «any use of apps and data should respect data security and EU fundamental rights, such as privacy and data protection» (Kędzior, 2020, p. 535).

1. Digital technologies and data have a valuable role to play in combating the COVID-19 crisis, given that many people in Europe are connected to the internet via mobile devices. Those technologies and data can offer an important tool for informing the public and helping relevant public authorities in their efforts to contain the spread of the virus or allowing healthcare organisations to exchange health data. However, a fragmented and uncoordinated approach risks hampering the effectiveness of measures aimed at combating the COVID-19 crisis, whilst also causing serious harm to the single market and to fundamental rights and freedoms (Recital 2).

2. National health authorities supervising infection transmission chains should be able to exchange interoperable information about users that have tested positive with other Member States or regions in order to address cross-border transmission chains (Recital 19).

3. Certain Member States have taken measures to simplify access to necessary data. However, the EU's common efforts combating the virus are hampered by the current fragmentation of approaches (Article 22).

In this contingency, measures should be «the least intrusive yet effective» (Article 16.2) for *epidemiological surveillance* (seven occurrences). Contact tracing apps should be *voluntary*, transparent, temporary, cybersecure, use temporary and pseudonymised data, rely on Bluetooth technology, be approved by national health authorities and be interoperable across borders as well as across operating systems (Bincoletto, 2021) in order to ensure respect for fundamental rights and prevent *stigmatization* (Article 16.1).

Recommendation 2020/518 was accompanied by the European Commission's Guidance on Apps that points out in detail how digital surveillance should be handled with full respect for data protection.

4. [*Apps*] can have a significant impact on disease diagnosis, treatment and management of COVID-19 inside and outside the hospital setting. They are particularly relevant when containment measures are lifted and when the risk of infection grows as more and more people are in contact with each other. These applications can help to interrupt infection chains faster and more efficiently than general containment measures, and can reduce the risk of the virus spreading significantly (EC, 2020b, p. 1).

5. The elements presented below aim to provide guidance on how to limit the intrusiveness of the app functionalities in order to ensure compliance with the EU personal data protection and privacy legislation (EC, 2020b, p. 2).

In fact, the effectiveness of contact tracing apps, which have repeatedly been accused of intrusive surveillance, has been questioned throughout. They were developed to trace cross-border infection chains and thus lift containment measures, but a preliminary evaluation shows that their usefulness has been limited, with findings on their effectiveness diverging significantly from country to country (Cebrian, 2021; Chiusi, 2021; Poillot *et al*., 2021).

At this point, the 2021 *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR* can be seen as a comprehensive report on the EU's legal framework and governance of health data, especially as «the onset of the pandemic has made it even more necessary to rethink the availability and accessibility of data and […] health data are needed in the fight against the virus and the protection against serious cross-border health threats in general» (EC, 2021, p. 53). The report outlines the features of the future European Health Data Space (EHDS).

6. the EHDS will provide access to datasets necessary to make successful use of emerging *responsible, human centred artificial intelligence and machine learning techniques* to drive innovation in healthcare (EC, 2021, p. 11, *emphasis added*).

As can be seen in the above quotation, the ethical concept of responsibility guides the digital governance of healthcare data by positioning artificial intelligence and big data as drivers for innovation within human control.

The *Assessment* dedicates an entire paragraph (4.5) to *public health threats* (12 occurrences) and their new trends (possibly new variants of the Coronavirus). Quite significantly, it points out to a fragmentation of approaches to these threats that are not just technical but legal, as inter-jurisdictional research highlights.

7. While the GDPR harmonises cross-European data protection law to facilitate the free flow of data across Member States, it is evident from the mapping of Member States' legislation and feedback from national experts, that there are divergences in the application of the GDPR in the context of health research (EC, 2021, p. 73).

8. While the GDPR is a much appreciated piece of legislation, variation in application of the law and national level legislation linked to its implementation have led to a fragmentation

of the law which makes cross-border cooperation for care provision, healthcare system administration or research difficult (EC, 2021, p. 144).

Shared ethical standards are especially important at the level of requirements for health-related research, as the data involved in that kind of practice are not only personal but sensitive. These concerns are diversely framed in the *Assessment* as *ethical evaluation, acceptability and supervision of biomedical research, ethical vetting, clear ethical and legal guidelines on how to use genomic data,* and *the ethical challenges of using private clouds for genetic research*.

The 2021 *Assessment* ends on a mention of trust and links it to patients' agency and rights in healthcare and cross-border healthcare, after noting at the beginning that «patients do not always find it easy to exercise the rights granted by the GDPR» (EC, 2021, p. 10).

9. [S]ound health data governance will be one of the pillars of trust that support the European Health Data Space, but it can only be successful if it is truly supportive of the other pillars of trust which demand assurance of data quality, transparency, and the full support to patients to act as active agents in their own health and care, with full capacity to exercise their health data related rights (EC, 2021, p. 145, *emphasis added*).

This is a central point in the EU's approach to digital governance and AI. Citizens should actively decide by free consent who can use their data and for what purposes, combined with *trustworthy* technologies, processes and actors.

In a similar manner, the eHealth Trust Framework «defines the rules, policies, protocols, formats and standards needed to ensure that Covid-19 health certificates are issued in such a way that their authenticity and integrity can be verified and trusted» (eHealth Network, 2021, p. 3). It amounts to saying that the certificate has been issued by an authorised entity, can be linked to the holder of the certificate and the information it presents is authentic, valid, and has not been altered. Once implemented at a national level, these certificates should be interoperable. Besides, the trust architecture that presides over the processing of personal data is also subject to legal considerations under the scope of the GDPR.

10. The trust framework should *by design and default* ensure the security and the privacy of data in the compliant implementations of digital vaccination certificate systems, ensuring both security and privacy (eHealth Network, 2021, p. 5).

In sum, benefits and challenges of health datafication as a central strategy in EU public health policy have increasingly gained visibility in institutional and legal communication, with the pandemic acting as a spur towards effective harmonisation and interoperability.

CONCLUSIONS

Following a number of legal regulations and policy decisions over the years, the Digital Agenda for Europe has established secure and shareable health data as a priority. Technical and legal interoperability between health data repositories is therefore of enormous importance to the overall public good and in public health. As such, in the EU official documents here illustrated, we observe that interoperability is discursively encoded through a number of words and phrases that aim to strike a balance between epidemiological surveillance and data protection.

However, these commitments did not fully hold up in practice in the COVID-19 health crisis. «It is a fundamental finding that the outbreak of the COVID-19 pandemic has revealed and exacerbated vulnerabilities in a wide variety of issues and areas» (Council of the European Union, 2020, p. 1). The health emergency has shown a number of possible obstacles to a more harmonised approach towards fighting the pandemic in the EU Member States. Once more, the pandemic has revealed how decentralised and disconnected Member States are from one another when it comes to healthcare, throwing into relief the importance of handling data efficiently to protect citizens (OECD, 2019).

Health datafication is still managed unevenly between them or within national health systems themselves. As fragmentation results in lower healthcare quality, and higher risk in controlling a pandemic, interoperability and standardisation should replace siloed technology.

Institutional communication about datafication in EU public health policy over the time span of a decade, but especially during and just after the pandemic, illustrates that regulations and guidelines hardly provide a straightforward answer. Instead, handling health data raises epistemological and ethical issues. Epistemologically, the digital governance of data is frequently prone to wrong assumptions.

The tendency to rely on mere Big Data furthermore ignores the variable quality of datasets. For instance, electronic health records typically consist of data written by clinicians for clinical work without the interests of researchers, standardisation and interoperability in mind, while aggregation of observational data for purposes of identifying causal links is prone to selection, confounding and measurement biases (Mittelstadt & Floridi, 2016, p. 18).

Nor can a tech solutionist position work satisfactorily at the ethical level. European societies are highly diversified, with an ageing population and uneven digital literacy. Too often in institutional discourse, citizens are framed «as rights holders …[*under*] the assumption that people are aware of their rights and can act upon that awareness» (Xenitidou & Gunnarsdóttir, 2019, p. 296). Conflicts of interest exist between connectedness and proprietary systems, risk factors should be evaluated to find a balance in the trade-off of civil liberties for safety (Akinsanmi & Salami, 2021), especially in the implementation of AI techniques and in machine learning. Innovative technologies are much needed for cost-effective and sustainable solutions in healthcare management and may be of great help during public health crisis, but they should also be trustworthy and allow for active consent. It follows that reliance on legal regulation should be enriched with insights from information ethics (Raab, 2017; Taylor, Floridi & van der Sloot, 2017). For Mittlestadt and Floridi (2016), the ethical mindset best suited for the governance of the digital in the EU is a «*post- compliance ethics*» (p. 4) or a «soft ethics approach» (p. 5), as in the EU «digital regulation is already on the good side of the moral vs. immoral divide» while «legislation is necessary but insufficient» (p. 5).

All these observations should be kept in mind while assessing the limited effectiveness of contact tracing applications in the COVID-19 pandemic, instead of dismissing this technology as an example of unsuccessful health datafication in the EU. Finally, digitising health records and enabling their exchange could also support the creation of large health data structures which can support the search for scientific discoveries, when combined with the use of new technologies, such as big data analytics and artificial intelligence.

REFERENCES

Akinsanmi, T & Salami, A. (2021). Evaluating the Trade-off between Privacy, Public Health Safety, and Digital Security in a Pandemic. *Data & Policy*, *3*(e27). https://doi.org/10.1017/dap.2021.24.

Bincoletto, G. (2020). Data Protection Issues in Cross-border Interoperability of Electronic Health Record Systems within the European Union. *Data & Policy 2*(e3), 1-11. https://doi.org/10.1017/dap.2020.2.

Cebrian, M. (2021). The Past, Present and Future of Digital Contact Tracing. *Nature Electronics 4*, 2-4. https://doi.org/10.1038/s41928-020-00535-z.

Chiusi, F. (2021). Digital Contact Tracing Apps: Do They Actually Work? A Review of Early Evidence. https://algorithmwatch.org/en/analysis-digital-contact-tracing-apps-2021.

Council of the European Union (2020). Council Conclusions on COVID-19: Lessons Learned in Health. 2020/C 450/01. *Official Journal of the European Union 450* (28.12.2020), 1-8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XG1228(01).

eHealth Network (2021). Interoperability of Health Certificates: Trust Framework. 12 March. https://eufordigital.eu/ehealth-network-event-focuses-on-covid-19-response-measures.

European Commission (2019). Commission Recommendation (EU) 2019/243 of February 6, 2019 on a European Electronic Health Record Exchange Format (C/2019/800). *Official Journal of the European Union 39* (11.2.2019), 18-27. http://data.europa.eu/eli/reco/2019/243/oj.

European Commission (2020a). Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data (C/2020/3300). *Official Journal of the European Union 114* (14.4.2020), 7-15. http://data.europa.eu/eli/reco/2020/518/oj.

European Commission (2020b). Guidance on Apps supporting the fight against COVID-19 pandemic in relation to data protection (C/2020/2523). *Official Journal of the European Union 124* (17.04.2020), 1-9, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020XC0417(08).

European Commission (2021). *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR* (11.2.2021). Luxembourg: Publications Office of the European Union.

European Commission Website (n.d). Public Health. Electronic Cross-Border Health Services. https://ec.europa.eu/health/ehealth-digital-health-and-care/electronic-cross-border-health-services_en.

European Parliament & Council of the European Union (2011). Directive 2011/24/EU of the European Council and of the Parliament of 9 March 2011 on the Application of Patients' Rights in Cross-Border Healthcare. *Official Journal of the European Union*, *88* (4.4.2011), 45-65. https://eur-lex.europa.eu/eli/dir/2011/24/2014-01-01.

Floridi, L. (2018). Soft Ethics and the Governance of the Digital. *Philosophy & Technology, 31*, 1-8. https://doi.org/10.1007/s13347-018-0303-9.

General Data Protection Regulation (GDPR) (2016). Regulation (EU) 2016/679. *Official Journal of the European Union, 119* (4.5.2016), 1-88. http://data.europa.eu/eli/reg/2016/679/oj.

Kędzior, M. (2021). The Right to Data Protection and the COVID-19 Pandemic: The European Approach. *ERA Forum 21*, 533-543. https://doi.org/10.1007/s12027-020-00644-4.

Martins, H. (2021). *EU Health Data Centre and a Common Data Strategy for Public Health*. Brussels: European Parliamentary Research Service (EPRS). https://www.europarl.europa.eu/stoa/en/document/EPRS_STU(2021)690009.

Mittelstadt, B. & Floridi, L. (2016). The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. *Science and Engineering Ethics 22*, 303-341. https://doi.org/10.1007/s11948-015-9652-2.

Morley, J., Cowls, J., Taddeo, M., & Floridi, L. (2020). Ethical Guidelines for COVID-19 Tracing Apps. *Nature*. https://www.nature.com/articles/d41586-020-01578-0.

OECD (2019). *Health in the 21st Century: Putting Data to Work for Stronger Health Systems*. OECD Health Policy Studies. Paris: OECD Publishing. https://doi.org/10.1787/e3b23f8e-en.

Paganoni, M.C. (2019). *Framing Big Data: A Linguistic and Discursive Approach.* Cham: Springer Nature/ Palgrave Macmillan.

Paganoni, M.C. (2020). Legal and Ethical Issues in Big Data Discourse. In: G. Tessuto, V.J. Bhatia, R. Breeze, N. Brownlees, & M. Solly (Eds.), *The Context and Media of Legal Discourse*, Legal Discourse and Communication Series (pp. 100-115). Newcastle upon Tyne: Cambridge Scholars Publishing.

Poillot, E., Lenzini, G., Resta, G., & Zeno-Zencovich, V. (2021). *Data Protection in the Context of COVID-19: A Short (Hi)story of Tracing Applications.* Rome: Roma Tre Press.

Raab, C.D. (2017). Information Privacy: Ethics and Accountability. In: C. Brand, J. Heesen, B. Kröber, U. Müller & T. Potthast (Eds.) *Ethik in den Kulturen – Kulturen in der Ethik*. Tübingen: Narr Franck Attempto, 335-347.

Refined eHealth European Interoperability Framework (ReEIF) (2015) https://ec.europa.eu/health/sites/default/files/ehealth/docs/ev_20151123_co03_en.pdf.

Tannen, D., Hamilton, H. E. & Schiffrin, Deborah (Eds.) (2015). *The Handbook of Discourse Analysis.* Second edition. Oxford: Wiley Blackwell.

Taylor, L., Floridi, L. & van der Sloot, B. (Eds.) (2017). Group Privacy: New Challenges of Data Technologies. Cham: Springer.

Xenitidou, M., & Gunnarsdóttir, K. (2019). The Power of Discourse: How Agency Is Constructed and Constituted in Discourse of Smart Technologies, Systems and Associated Developments. *Discourse & Society 30*(3), 287-306. https://doi.org/10.1177/0957926519828031.