The GDPR and (Big) Health Data: Assessing the EU Legislator's Choices

Dr. Maria Tzanou, Senior Lecturer in Law, Keele University, UK

ORCID: 0000-0001-5360-2038

Abstract

This chapter critically examines the GDPR's provisions relating to health by focusing on two main issues: i) the definitional uncertainties surrounding health data and, ii) the legislative choices regarding the balance between the competing interests to data privacy on the one hand -seen mainly within the context of the enhanced protection that personal health data enjoy-, and the interests of 'public health' on the other hand. I argue that while the GDPR's provisions balancing data privacy with public health interests appear flexible and context- dependent, its binary definitional distinctions (sensitive (health)/ non-sensitive (non-health) data is problematic and may result in rendering the GDPR's rules both over- and under- inclusive.

1. Introduction

The COVID-19 pandemic has not only created an unprecedented health emergency in modern times across the globe; it has also brought forward a variety of data privacy issues. Imposed lockdowns, quarantines and 'self-isolation' measures are examples of what Anita Allen has coined as 'unpopular privacy'.[1] 'Unpopular privacy' refers to coercive mandates that 'impose unpopular privacies on intended targets and beneficiaries' just like the COVID-19 related social distancing rules.[2] Schools and workplaces are closed; public events are cancelled; the

[1] Anita L. Allen, *Unpopular Privacy: What Must We Hide?* (Oxford University Press, New York, 2011).
[2] Ibid.

use of public transport is limited;[3] people are even forbidden to do normal everyday activities,[4] such as sunbathing.[5] At the same time and in order to combat this pandemic, whole populations are required to endure increased surveillance of their location, their movements and their contacts[6] via the invasive monitoring of mobile phone data.[7]

Widespread health data surveillance is not a new phenomenon. Health data and the capture of their enormous potential through big data analytics have been at the forefront of recent debates, before the emergence of a global health pandemic. Data privacy regulatory responses to health data surveillance vary around the world, but the EU's General Data Protection Regulation ('GDPR')[8] with its strengthened data privacy rules and principles remains a point of reference. This chapter critically examines the GDPR's provisions relating to health by focusing on two main issues: i) the definitional uncertainties surrounding health data and, ii) the legislative choices regarding the balance between the competing interests to data privacy on the one hand -seen mainly within the context of the enhanced protection that personal health data enjoy-, and the interests of 'public health' on the other hand.

The analysis proceeds as follows: The following Section assesses the definitional uncertainties that big health data raise. It takes a closer look at big data analytics and the sources

[3] For an overview of COVID-19 restrictive measures across the world, see Oxford University's COVID-19 Government Response Tracker project. Hale Thomas et al., Oxford COVID-19 Government Response Tracker, (2020) Blavatnik School of Government. Data use policy: Creative Commons Attribution CC BY standard < https://www.bsg.ox.ac.uk/research/research-projects/oxford-covid-19-government-response-tracker>.
[4] See also Rebecca Ratcliffe, 'Teargas, beatings and bleach: the most extreme Covid-19 lockdown controls around the world', *The Guardian*, 1 April 2020 < https://www.theguardian.com/global-development/2020/apr/01/extreme-coronavirus-lockdown-controls-raise-fears-for-worlds-poorest>.
[5] Alison Hills, '"Can I sunbathe in the park?" is now a deep moral question', *The Guardian*, 10 April 2020 < https://www.theguardian.com/commentisfree/2020/apr/10/sunbathing-park-deep-moral-questions-philosophers-coronavirus-individual>.
[6] Jack Nicas and Daisuke Wakabayashi, 'Apple and Google Team Up to "Contact Trace" the Coronavirus', *The New York Times*, 10 April 2020 < https://www.nytimes.com/2020/04/10/technology/apple-google-coronavirus-contact-tracing.html> .
[7] Alex Hern, 'Experts warn of privacy risk as US uses GPS to fight coronavirus spread', *The Guardian*, 2 April 2020 < https://www.theguardian.com/technology/2020/apr/02/experts-warn-of-privacy-risk-as-us-uses-gps-to-fight-coronavirus-spread> .
[8] 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 (General Data Protection Regulation), Official Journal of the European Union , L 119/1, 4 May 2016.

of big health data and examines definitional questions within the GDPR's context. Section 3 discusses the GDPR's legislative choices regarding health data by focusing on their enhanced protection as 'special categories of data' and the exemptions and restrictions imposed on these for public health purposes. Section 4 offers brief Conclusions.

2. On Definitional Issues: What is Big Health Data?

2.1 Big data analytics

We are living in a big data world. Every minute 510,000 comments are posted on Facebook, 293,000 statuses are updated, and 136,000 photos are uploaded. 3.5 billion Google searches are made every day; 6,000 tweets are sent per second; more than 95 million photos and videos are uploaded on Instagram per day. There are 3.3 billion smartphone users worldwide and the average smartphone user has 60 and 90 apps on their device[9] collecting some kind of personal data (i.e, name, e-mail address, location).[10] Outside the online world, the Internet of Things (IoT) 'merges physical and virtual worlds'[11] through a range of interconnected devices[12] that communicate data, such as smart thermostats, meters, doorbells, smoke alarms, cameras, digital assistants, TVs and fridges. [13] According to the European Commission, the value of

[9] Gillian Cleary, Mobile Privacy: What Do Your Apps Know About You?, 16 August 2018 < https://www.symantec.com/blogs/threat-intelligence/mobile-privacy-apps>.
[10] Art 29WP Opinion 02/2013 on apps on smart devices, WP 202, Adopted on 27 February 2013.
[11] European Commission, Digital Single Market Policy- The Internet of Things < https://ec.europa.eu/digital-single-market/en/internet-of-things> .
[12] The European Commission estimates that the number of IoT connections will raise to 6 billion by 2020. Commission Staff Working Document, Advancing the Internet of Things in Europe, Accompanying the document Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Digitising European Industry Reaping the full benefits of a Digital Single Market {COM(2016) 180 final}, Brussels, 19.4.2016 SWD(2016) 110 final. See also, Art 29 WP, *Opinion 8/2014 on Recent Developments on the Internet of Things*, adopted on 16 September 2014; Samuel Greengard, *The Internet of Things* (MIT Press, 2015).
[13] Kari Paul, Teen claims to tweet from her smart fridge – but did she really?, 13 August 2019 < https://www.theguardian.com/technology/2019/aug/13/teen-smart-fridge-twitter-grounded>.

European citizens' personal data has the potential to grow to nearly €1 trillion annually by 2020.

There is not a commonly agreed definition of big data.[14] In broad terms, big data refers to the aggregation of huge volumes of diversely sourced information and their analysis, using sophisticated algorithms to inform decisions.[15] Big data is made possible due to the increasing capabilities of technology to support the collection and storage of large amounts of data, as well as 'its ability to analyse, understand and take advantage of the full value of data (in particular using analytics applications)'.[16] Big data is often described using the five V's: Volume, Variety, Velocity, Veracity, and Value.[17] Volume refers to the expanding amounts of data generated and the large-scale datasets; Variety relates to the different types of data and data sources; Velocity describes both the increasing speed at which data is produced and the increasing demand to analyse the data in near real time to get insights; Veracity[18] refers to the correctness and accuracy of the data; and, Value denotes the opportunities of big data to lead to measurable improvements of our lives.[19]

Perhaps the most important characteristic of big data refers to the ways this is analysed. The full potential of big data can be realised using AI.[20] AI is needed to 'mine, parse, sort and

[14] On the meaning of 'data' and 'information' in the law in general and in data protection laws see Lee Bygrave, 'Information Concepts in Law: Generic Dreams and Definitional Daylight', (2015) 35 (1) *Oxford Journal of Legal Studies*, 91.
[15] EDPS, Opinion 7/2015 *Meeting the challenges of big data- A call for transparency, user control, data protection by design and accountability*, 7.
[16] Ibid.
[17] Kitchin argues that there are seven dimensions to big data, including exhaustivity, resolution and indexicality, relationality and extensionality and scalability. Rob Kitchin, *The Data Revolution: Big Data, Open Data, Data Infrastructures and their Consequences* (Sage, 2014). Rob Kitchin and Gavin McArdle, 'What makes big data, big data? Exploring the ontological characteristics of 26 datasets' (2016) 3 (1) *Big Data and Society*, 1.
[18] Variability is also often mentioned. This means that data captured may vary from time to time or place to place. Anil Jain, The 5 V's of big data, 17 September 2016 < https://www.ibm.com/blogs/watson-health/the-5-vs-of-big-data/>.
[19] Sander Klous, Sustainable harvesting of the big data potential in Bart van der Sloot et al. (eds.) *Exploring the boundaries of big data* (Amsterdam University Press, Amsterdam 2016), 27, 28.
[20] UK Government Office for Science, *Artificial intelligence: opportunities and implications for the future of decision making*, 9 November 2016, 5.

configure the data into useful packages',[21] build models and draw inferences that are then used 'to predict and anticipate possible future events'.[22] This is often done through machine learning, namely 'algorithms that change in response to their own output, or "computer programs that automatically improve with experience".'[23] Machine learning means that the system is able to train itself to learn continuously and modify its behaviour during operation, thus acquiring a level of autonomy.[24] Big data, AI and machine learning are closely related concepts and sometimes are referred to interchangeably. However, there are differences between the two. As the UK Government Office for Science astutely puts it: 'If data is the fuel, artificial intelligence is the engine of the digital revolution'.[25] As it might be more accurate in terms of terminology to use the umbrella concept 'big data analytics' to describe all the three of them.[26] That being said, this chapter and this book understands 'big data' as 'big data analytics' and the two terms are used interchangeably.

2.2 Big health data

Health data are at the centre of the big data revolution. Over 250,000 health and fitness apps are currently available on the market. The sale of wearables, such as smart watches, fitness trackers, eye gears, smart clothing, smart jewellery and implantables is on the rise with more

[21] John Danaher et al., 'Algorithmic governance: Developing a research agenda through the power of collective intelligence', (2017) *Big Data & Society*, 1, 2.
[22] UK Government Office for Science, n 20, 5.
[23] Ibid, 6.
[24] Ibid, 7.
[25] Ibid, 4.
[26] Information Commissioner's Office (ICO), *Big data, artificial intelligence, machine learning and data protection*, 20170904 Version: 2.2, para 11.

than 170 million wearables being purchased in 2018.[27] There are 'vagina fitbits',[28] smart vibrators, smart nappies,[29] and smart baby socks that measure babies' 'temperature, heart rate, oxygen saturation and movement'[30] available on the market. Our bodies emit streams of data: everything from physical activity, calorie intake, sleep, posture to sexual intercourse, menstrual cycles, fertility and breathing patterns can be (self)-tracked, measured, logged and (self)-analysed in order to achieve 'self-knowledge through numbers'.[31] The observation of our bodies through technologies is ingrained in our everyday lives and global trends such as the Quantified-Self are constantly growing.[32] Platforms like PatientsLikeMe enable the exchange of information about illnesses creating 'a community of people who are helping each other live their best every day'.[33] According to PatientsLikeMe, over '650,000 people living with 2,900 conditions have generated more than 43 million data points, creating an unprecedented source of real-world evidence and opportunities for continuous learning.'[34]

Big health data analytics promise a number of benefits. Indeed, the convergence between technology and healthcare is expected to: i) increase quality of life and contribute to disease prevention[35] and, therefore, reduce healthcare expenditure[36] ii) allow 'better healthcare

---

[27] Sarah Perez, IDC: Apple led wearables market in 2018, with 46.2M of the total 172.2M devices shipped, 5 March 2019 < https://techcrunch.com/2019/03/05/idc-apple-led-wearables-market-in-2018-with-46-2m-of-the-total-172-2m-devices-shipped/>.

[28] Oliver Wainwright, 'KGoal: introducing the fitness tracker for your vagina', *The Guardian*, 4 July 2014 < https://www.theguardian.com/artanddesign/architecture-design-blog/2014/jul/04/kgoal-fitness-tracker-vagina-pelvic-floor> .

[29] Arwa Mahdawi, 'Is buying a 'smart nappy' really such a clever idea?', *The Guardian*, 24 July 2019 < https://www.theguardian.com/commentisfree/2019/jul/24/is-buying-a-smart-nappy-really-such-a-clever-idea?CMP=Share_AndroidApp_Gmail> .

[30] Richard Godwin, '"You can track everything": the parents who digitise their babies' lives', *The Guardian*, 2 March 2019 < https://www.theguardian.com/lifeandstyle/2019/mar/02/apps-that-track-babies-and-give-data-to-tech-firms-parents> .

[31] See Quantified Self- Self Knowledge Through Numbers < https://quantifiedself.com/>.

[32] Deborah Lupton, *The Quantified Self* (Polity Press, 2016).

[33] See https://www.patientslikeme.com/about.

[34] Ibid. 'Today, PatientsLikeMe is the world's largest personalized health network…Everything members have shared empowers the community with personal agency, establishing PatientsLikeMe as a clinically robust resource that has published more than 100 research studies.'

[35] European Commission, Green Paper on mobile Health ("mHealth"), Brussels, 10.4.2014, COM(2014) 219 final, 4.

[36] Deborah Lupton, 'Quantifying the Body: Monitoring and Measuring Health in the Age of mHealth Technologies', (2013) 23(4) *Critical Public Health*, 393

at a lower cost', iii) foster 'patient empowerment (i.e. improved control over own healthcare)', iv) enable 'easier and more immediate access to medical care and information online',[37] and v) develop 'more efficient and sustainable healthcare'.[38] Algorithmic analysis of huge datasets will develop 'personalised medicine' based on more accurate diagnostic predictions and treatment suggestions.[39] Such improvements are not an issue of the future; they are happening right now. Deep learning AI is already 'on a par with human experts'[40] when it comes to making medical diagnoses of diseases from cancers to eye conditions[41] based on images, and it might soon outperform humans. Big data analysis allows the discovery of previously unknown trends, correlations and patterns and, therefore, offers new valuable insights for medical research.[42]

2.3 On definitional uncertainties: What is 'big' 'health' data?

Big health data are generated in mass and offer significant promises to improve our wellbeing and healthcare. If, therefore, we are to study carefully the challenges the immense datafication of our bodies is posing and the ways the law can approach these, we need first to define what 'health data' and 'big health data' means.

---

[37] EDPS, Opinion 1/2015 *Mobile Health: Reconciling technological innovation with data protection*, 21 May 2015, 3.
[38] Commission, Green Paper on mHealth, n 35, 5.
[39] Kate Crawford and Jason Schultz, 'Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms', (2014) 55 *B.C.L. Rev*., 93, 102 < http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4 >.
[40] Nicola Davis, 'AI equal with human experts in medical diagnosis, study finds', The Guardian, 24 September 2019, < https://www.theguardian.com/technology/2019/sep/24/ai-equal-with-human-experts-in-medical-diagnosis-study-finds?CMP=Share_AndroidApp_Gmail> .
[41] Ian Sample, ''It's going to create a revolution': how AI is transforming the NHS', The Guardian, 4 July 2018, < https://www.theguardian.com/technology/2018/jul/04/its-going-create-revolution-how-ai-transforming-nhs> .
[42] EDPS, Opinion 1/2015 *Mobile Health*, n 37, 9.

Unlike its predecessor (the Data Protection Directive[43]), the GDPR contains a definition of 'data concerning health'. This can serve as a starting point for the present analysis. According to the GDPR, 'data concerning health' refers to '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.' [44] Recital 35 further explains that 'personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU[45]…to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.' 'Genetic data' as defined in the GDPR is also relevant to health data. The GDPR defines 'genetic data' as 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the *health* of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question'.[46]

[43] Directive 95/46/EC 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, OJ L 281, 23/11/1995, p. 31.
[44] Article 4 (15) GDPR.
[45] 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, OJ L 88, 4.4.2011, p. 45.
[46] Article 4 (13) GDPR. Emphasis added.

The definition of 'health data' is not without problems. First, it appears tautological; it is not clear what is personal data related to the 'physical or mental health' or data that reveals information about a person's 'health status'. The GDPR does not define what constitutes 'health' although this appears several times in this legislative instrument in different combinations: 'health status', 'public health', 'health purposes', 'health insurance', 'health security'. Nevertheless, it should be acknowledged that the definition of 'data concerning health' in the GDPR is quite broad. It includes healthcare data referring to medical history, diseases and disability, but also information about the past, current and future health status of the data subject including disease risk.

The big data context complicates things even further. What about data generated outside the health care setting, for instance, fitness and well-being data captured through wearables and fitness apps? Are these considered 'health data'? Completely trivial and innocuous data, such as supermarket shopping lists may also reveal information about a person's dietary habits and, consequently, their health status. Indeed, it has been argued that a supermarket shopping database can be used to determine a 'person's current and future health status with a degree of accuracy comparable to that of a medical examination' with the ability to 'detect individuals' propensity to develop diseases such as diabetes, women's cancers, smoking-related cancers, cardiovascular disease, depression, etc'.[47] Furthermore, what constitutes health information can be context-dependent; a piece of information might not possess the 'intrinsic nature'[48] of health data, but, analysed by algorithms it might reveal the health status of a person. The often cited by privacy scholars case of the department store Target sending to a teenage girl ads about pregnancy products -before her family knew of her pregnancy- on the basis of her purchasing certain goods, such as lotions and vitamin

[47] Antoinette Rouvroy, '"Of Data and Men" Fundamental Rights and Freedoms in a World of Big Data', Bureau of the Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [ETS 108], p. 27.
[48] EDPS, Opinion 1/2015 *Mobile Health*, n 37, 6.

supplements,[49] demonstrates the potential of big data analytics. Definitional difficulties are exacerbated in the big data environment because data are not static, but dynamic; at one time point, they might be irrelevant to health -or even not personal data at all- (for instance, the levels of environmental pollution, weather data[50]) and at the next moment, combined and analysed with other datasets (i.e, lifestyle habits), they might reveal sensitive information.

It is not only that the meaning of 'health data' is blurred. Uncertainties also arise as to what constitutes 'big (health) data'. First, the term 'big' can be misleading in different ways.[51] The data is not always 'big'; it's their aggregation and analysis that matters. As Zuboff observes, '"big data" are constituted by capturing small data from individuals' computer-mediated actions and utterances in their pursuit of effective life. Nothing is too trivial or ephemeral for this harvesting: Facebook "likes", Google searches, emails, texts, photos, songs, and videos, location, communication patterns, networks, purchases, movements, every click, misspelled word, page view, and more. Such data are acquired, data*fi*ed, abstracted, aggregated, analysed, packaged, sold, further analysed and sold again.'[52] It's not only that 'big data' is made by bits of 'small data'. It is also 'not always easy (or indeed useful) to say whether a particular instance of processing is or is not big data analytics.'[53] As technologies and algorithmic tools are increasingly ingrained in our lives, big data analytics are becoming the new normal, a part 'of business as usual'.[54]

---

[49] Kashmir Hill, 'How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did', *Forbes*, 16 February 2012 < https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#d4fc43566686> .

[50] Mr Dehaye, a Belgian national, received an email from The Weather Company, owned by IBM that informed him that 'based on hot weather conditions in Mr Dehaye's area he was likely to have an "overactive bladder" — and buy more drinks' 9 June 2019. See Aliya Ram and Madhumita Murgia, 'Data brokers: regulators try to rein in the "privacy deathstars"', *Financial Times,* 8 January 2019, < https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521> .

[51] See Matthew Jones, 'What we talk about when we talk about (big) data' (2019) 28 *Journal of Strategic Information Systems*, 3. Jones argues that '[r]ather than being a referential, natural, foundational, objective and equal representation of the world, …, data are partial and contingent and are brought into being through situated practices of conceptualization, recording and use.'

[52] Shoshana Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization', (2015) 30 *Journal of Information Technology*, 75, 79.

[53] ICO, *Big data, artificial intelligence, machine learning and data protection*, n 26, 13.

[54] Ibid.

Overall, the definitional boundaries of 'big health data' are not clear cut. What is 'big' data/ what is 'small' data; what is 'health' data/ what is not health data; what is personal data/ what is non-personal data; what is 'big data analytics' and what business as usual may differ from time to time and from context to context. The implications of these definitional uncertainties matter for this book. The GDPR considers 'data concerning health' as special categories of data (normally referred to as sensitive data) that merit enhanced protection.[55] Yet, the definitional difficulties discussed above cannot be resolved by merely construing 'health data' broadly as proposed by the EDPS.[56] They demand a shift in thinking that can approach the problem in a novel, dynamic way that addresses the big data context.

That being said, this book adopts in general the not so accurate terminology of 'big health data' or 'big health data analytics' as an umbrella concept that covers broadly data generated from a variety of different sources and from which information about a person's health can be inferred. Some chapters focus on what can be seen as 'small' data instances of processing (such as sharenting), not losing sight of the fact, however, that any information however small can be potentially rendered big data.[57]

2.4 Sources of big health data

Big health data can be captured in a variety of ways: i) it can be volunteered or surrendered by individuals when they share information about themselves (e.g. patient data shared with healthcare professionals) or third parties (e.g. their children); ii) monitored by tracking their activities (e.g. Google searches, loyalty schemes in gyms that record attendance, supermarkets

[55] See Art 9 GDPR.
[56] EDPS, Opinion 1/2015 *Mobile Health*, n 37, 6.
[57] Helen Nissenbaum has stated 'anything about an individual that can be rendered in digital form can be stored over indefinitely long periods and be readily retrieved.' See Helen Nissenbaum, 'Privacy as Contextual Integrity', (2004) 79 *Wash. L. Rev.* 119, 129.

that record purchasing history); and, finally it can be 'inferred', based on the analysis or the 'profiling'[58] of volunteered, monitored and other data (e.g. health insurance premiums). [59] According to an OECD report, the big data 'lifecycle' often follows the follows sequence of steps: i) collection/ access; ii) storage and aggregation; iii) analysis and distribution; and, iv) usage.[60] Each step could potentially involve different stakeholders[61] and data could have several lifecycles entailing further aggregation and analysis.

There is a plethora of sources through which health information can be captured. Outside the traditional medical/ healthcare sector, *mhealth* is an important source of big health data. Mobile Health ('mHealth') broadly refers to mobile devices and applications ('apps') that deliver health, well-being and lifestyle services and information.[62] These include wearables -data collection devices worn on the body- (such as fitness trackers and smart watches) and health and fitness apps. mHealth solutions can be used to deliver a wide range of services,[63] including measure and quantify basic bodily functions (such as breathing rate, sleep, heart rate, blood pressure, blood glucose level) and habits (exercise patterns), offer medication reminders, fitness recommendations and nutritional advice, book medical appointments, assist users with health-related questions, etc. mHealth apps and devices routinely share users' data

[58] Recital 71 GDPR explains that profiling 'consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.' For further details on the challenges posed by profiling, see Tzanou's chapter in this book.

[59] OECD, 'Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value', (2013) OECD Digital Economy Papers, No. 220, OECD Publishing <http://dx.doi.org/10.1787/5k486qtxldmq-en >, 10.

[60] Ibid.

[61] Ibid.

[62] The Commission states that mHealth covers 'medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices. It also includes …lifestyle and wellbeing apps that may connect to medical devices or sensors (e.g. bracelets or watches) as well as personal guidance systems, health information and medication reminders provided by sms and telemedicine provided wirelessly.' See Commission, Green Paper on mHealth, n 35, 3.

[63] For a theoritisation of the mhealth phenomenon, see Lupton, n 36.

with third parties[64] such as advertisers. Apps can also be integrated with social media platforms in order to enhance users' experience by showcasing personal statistics and performances. Furthermore, wearables and apps can be used to facilitate 'gamification', understood as the 'use of game-like incentives'[65] (targets, competition) to encourage users to change their behaviour concerning physical activities[66] (i.e., walking) and even intimate relationships.[67]

mHealth devices and apps illustrate the potential of 'surveillance capitalism'.[68] As Lupton has noted

> These devices could ... be regarded as disciplinary, working to tame the …body by rendering it amenable to monitoring, tracking, and detailed analysis of the data thus generated… These technologies configure a certain type of approach to understanding and experiencing one's body, an algorithmic subjectivity, in which the body and its health states, functions and activities are portrayed and understood predominantly via quantified calculations, predictions and comparisons.'[69]

mHealth technologies are often connected to social media. for instance, a Fitbit can share the user's data on Facebook in order to showcase their performance. Social media platforms themselves contain important troves of health-related information. Facebook, Twitter,

---

[64] For a very interesting empirical study, see Quinn Grundy et al., 'Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis', (2019) 364: l920 *BMJ*, 1.
[65] John Danaher, Sven Nyholm and Brian D. Earp, 'The Quantified Relationship' (2018) *The American Journal of Bioethics*, 3.
[66] Ali Shameli et al., 'How Gamification Affects Physical Activity: Large-scale Analysis of Walking Challenges in a Mobile Application' (2017) *Proc Int World Wide Web Conf.*, 455; Rekesh Corepal et al., 'Exploring the use of a gamified intervention for encouraging physical activity in adolescents: a qualitative longitudinal study in Northern Ireland' *BMJ Open* 0:e019663.
2018
[67] Danaher et al., n 21.
[68] Shoshana Zuboff, 'Big other: surveillance capitalism and the prospects of an information civilization', (2015) 30 *Journal of Information Technology*, 75. See also Tereza Hendl, Bianca Jansky, and Verina Wild, 'From Design to Data Handling. Why mHealth Needs a Feminist Perspective' in Loh J. and Coeckelbergh M. (eds.) *Feminist Philosophy of Technology* (Techno:Phil – Aktuelle Herausforderungen der Technikphilosophie, vol 2. J.B. Metzler, Stuttgart, 2019), 77.
[69] Deborah Lupton, 'Quantified Sex: A Critical Analysis of Sexual and Reproductive Self-Tracking Using Apps' (2014) 17 *Culture, Health & Sexuality*, 440.

Instagram and PatientsLikeMe provide significant opportunities to form online communities - among others- also around health issues, but they have also increased the opportunities for health data surveillance.[70] For instance, PatientsLikeMe state that they share personal data, including information 'you provide about yourself to share with others like the condition you're living with and treatments you're trying' with the PatientsLikeMe community as well as with partners that include universities, pharmaceutical companies, hospital systems, insurance companies, regulatory bodies and 'members of the Digital Life Alliance — like-minded digital health, science, and technology companies who work closely with PatientsLikeMe to improve health and healthcare around the globe'.[71]

3. On legislative choices: GDPR and health

3.1 The GDPR: An Overview

The General Data Protection Regulation constitutes the centrepiece of EU data privacy law. The GDPR is a long and complex legislative document. It contains 173 (non-binding) Recitals and 99 provisions laying down 'rules relating to the protection of natural persons with regard to the processing[72] of personal data[73] and rules relating to the free movement of personal

[70] Frank Pasquale and Tara Adams Ragone, 'Protecting Health Privacy in an Era of Big Data Processing and Cloud Computing' (2014) 17 *STAN. TECH. L. REV.,* 595, 632.
[71] PatientsLikeMe Privacy Policy < https://www.patientslikeme.com/about/privacy> .
[72] According to Article 4 (2), 'processing' means 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction'.
[73] According to Article 4 (1), 'personal data' means 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'.

data'.[74] The GDPR does not apply to the processing of personal data that falls outside the scope of EU law; concerns national security policy; processing by a natural person in the course 'of a purely personal or household activity'; or processing for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[75]

In its substance, the GDPR is an omnibus regulation covering processing of personal data by both private and public bodies and addressing 'an immense landscape of potential informational problems'.[76] The provisions of the GDPR are structured around two main actors: the 'data subjects' and the 'controllers'. 'Data subjects' are the natural persons whose personal data are processed. 'Controllers' are the natural or legal persons, public authorities, or other bodies which, 'alone or jointly with others, determine the purposes and means of the processing of personal data'.[77] National Data Protection Authorities (DPAs) oversee the application of the GDPR.[78]

The GDPR is a 'principles-based regulation'.[79] It includes six principles on the basis of which personal data must be processed: 'lawfulness, fairness and transparency';[80] 'purpose

[74] Art 1 (1) GDPR.
[75] Art 2 (2) GDPR.
[76] Chris Jay Hoofnagle, Bart van der Sloot and Frederik Zuiderveen Borgesius, 'The European Union general data protection regulation: what it is and what it means', (2019) 28 (1) *Information & Communications Technology Law*, 65, 67.
[77] Art 4 (7) GDPR.
[78] See Article 51 GDPR.
[79] Hoofnagle, van der Sloot and Borgesius, n 76, 67.
[80] Article 5 (1) (a): Personal data should be 'processed lawfully, fairly and in a transparent manner in relation to the data subject'.

limitation';[81] 'data minimisation';[82] 'accuracy';[83] 'storage limitation';[84] and, 'integrity and confidentiality'.[85] An additional 'accountability' principle makes controllers responsible for complying with these data processing principles.[86]

Data subjects are granted a number of rights under the GDPR: a right of information,[87] access to,[88] rectification[89] and erasure[90] of personal data, a right to data portability,[91] a right to restrict[92] and object to certain types of processing,[93] and a right not to be subjected to fully automated decisions based on profiling.[94] Data breaches must be communicated by controllers to data subjects when they are likely to result in a high risk to the rights and freedoms of natural persons.[95]

The GDPR introduces a risk-based approach to data protection. Recital 75 explains that risks 'of varying likelihood and severity may result from personal data processing' and could lead to 'physical, material or non-material damage' and provides examples of such risk.[96]

---

[81] Article 5 (1) (b): Personal data should be 'collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes'.
[82] Article 5 (1) (c): Personal data should be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'.
[83] Article 5 (1) (d): Personal data should be 'accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay'.
[84] Article 5 (1) (e): Personal data should be 'kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed'.
[85] Article 5 (1) (f): Personal data should be 'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures'.
[86] Article 5 (2) GDPR.
[87] Articles 13 and 14 GDPR.
[88] Article 15 GDPR.
[89] Article 16 GDPR.
[90] Article 17 GDPR. Article 17 is entitled 'Right to erasure ("right to be forgotten").
[91] Article 20 GDPR.
[92] Article 18 GDPR.
[93] Article 21 GDPR.
[94] Article 22 GDPR.
[95] Article 34 (1) GDPR.
[96] The processing may give rise to 'discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; …data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; … personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal

Controllers are obliged to undertake *ex ante* data protection impact assessments (DPIAs)[97] 'where a type of processing in particular using new technologies, …is likely to result in a high risk to the rights and freedoms of natural persons',[98] and notify *ex post* data breaches to supervisory authorities and the data subject[99] when they are 'likely to result in a high risk to the rights and freedoms of natural persons'.[100]

3.2 Health data under the GDPR

The GDPR contains a number of provisions on health data and health. Besides the definitional issues seen above, these concern on the one hand, the enhanced protection of health data as 'special categories of personal data',[101] and, on the other hand, the exemptions and restrictions to data protection rules and principles for health reasons.

Health data enjoy increased levels of protection under the GDPR.[102] First, as a basic rule, the GDPR prohibits the processing of data concerning health.[103] There are several exceptions to this prohibition that will be discussed below.

Second, the GDPR considers the processing of health data -and sensitive data in general- as one that might pose a 'risk' to the rights and freedoms of natural persons.[104] More fundamentally, there are cases where the GDPR views personal health data processing as 'high-risk'. For instance, the GDPR recognises that a high risk to the rights and freedoms of natural

convictions and offences or related security measures; … personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; … personal data of vulnerable natural persons, in particular of children, are processed; or …processing involves a large amount of personal data and affects a large number of data subjects'.

[97] Articles 35, 36 GDPR and Recital 76. For an ethical and social impact assessment see Alessandro Mantelero, 'AI and Big Data: A blueprint for a human rights, social and ethical impact assessment' (2018) 34 *Computer Law & Security Review*, 754.

[98] Article 35 (1) GDPR.

[99] Articles 33 and 34 GDPR.

[100] Article 34 (1) GDPR.

[101] Article 9 GDPR.

[102] According to Recital 53 '[s]pecial categories of personal data… merit higher protection'.

[103] Article 9 (1) GDPR.

[104] Recital 75 GDPR.

persons might arise when health data are processed 'on a large scale'[105] and obliges controllers to carry out a DPIA in this context.[106] This would include the case where a large hospital processes patients' genetic and health data,[107] although the GDPR is careful to point out that the processing of personal data of patients by an individual physician or other health care professional would not be considered as 'large-scale'.[108]

Third, the GDPR prohibits automated decision-making including profiling,[109] which produces legal effects concerning a person or significantly affects her to be undertaken based on health data, unless the data subject has given her explicit consent or processing is necessary for reasons of substantial public interest and suitable measures to safeguard the data subject's rights, freedoms and legitimate interests are in place.[110] The GDPR grants data subjects the right not to be subject to fully automated decisions that analyse or predict aspects concerning their health[111] and obliges controllers to undertake a DPIA if they engage in such a systematic and extensive evaluation of natural persons based on automated processing, including profiling.[112]

Fourth, the GDPR specifically mentions the data subject's rights of information and access in relation to their health data. These include the right for data subjects to have 'access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided'.[113]

---

[105] Article 35 (3) (b) GDPR.
[106] Ibid. See also 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, WP248, 4 April 2017.
[107] Hoofnagle, van der Sloot and Borgesius, n 76, 87.
[108] Recital 91 GDPR.
[109] According to Article 4 (4) GDPR 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's … health...'
[110] Article 22 (4) GDPR.
[111] Recital 71 GDPR.
[112] Article 35 (3) (a) GDPR.
[113] Recital 63 GDPR.

Fifth, additional responsibilities are imposed on controllers processing health data: these must keep records of processing activities even if the organisation employs fewer than 250 persons;[114] they must designate a Data Protection Officer (DPO) if the core activities of the controller or the processor consist of processing health data on a large scale;[115] and, controllers and processors not established in the EU must designate in writing a representative in the Union if they process health data on a large scale.[116]

3.3 Exemptions allowing health data processing

The GDPR contains a number of exceptions to the (in principle) prohibition of processing of health data.[117] First, the processing of health data is allowed if the data subject has given her 'explicit consent'.[118] It should be recalled that the GDPR has significantly raised the substantive and procedural requirements on 'consent' for the processing of personal data in general;[119] the bar is even higher when special categories of data and, therefore, health data are at issue. The GDPR even allows Member States or the EU under certain instances to remove the consent exception altogether.[120]

Health data can also be processed when this is necessary to protect the 'vital interests' of the data subject or of another person when they are physically or legally incapable of giving their consent[121] (e.g. the data subject is unconscious after an accident, and the hospital needs to know her medical history, whether she has any allergies or uses any medication). Health data processing is further allowed where this has been 'manifestly made public by the data

[114] Article 30 (5) GDPR.
[115] Article 37 (1) (c) GDPR.
[116] Article 27 (2) (a) GDPR.
[117] Article 9 (2) GDPR. Only the ones most relevant to health data are discussed here.
[118] Article 9 (2) (a) GDPR.
[119] See Hoofnagle, van der Sloot and Borgesius, n 76, 72.
[120] Article 9 (2) (a) GDPR.
[121] Article 9 (2) (c) GDPR.

subject'.[122] This provision creates a number of uncertainties because as seen above mhealth apps and devices (such as Fitbits) often share users' information on social media and individuals frequently post health-related information in social media both generic (Facebook, Twitter, etc.) and specific ones (PatientsLikeMe). The GDPR seems to permit the processing of health data in this respect,[123] but I submit that the mere posting of health data in social media would not be enough to allow the processing of such data by another controller.

The processing of health data is also allowed when necessary for reasons of 'substantial public interest'.[124] It should be noted that the GDPR does not require the processing merely in the 'public interest'; the public interest must be 'substantial'. What constitutes 'substantial public interest' is not defined in the GDPR. Moreover, the GDPR allows the processing of health data when necessary 'for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services'.[125] Finally, the GDPR provides that Member States can maintain or introduce further conditions, including limitations, with regard to the processing of health, genetic data and biometric data.[126] This might contribute to the further fragmentation of the health data landscape in the EU and increase uncertainties.

3.4 'Public health' exceptions and restrictions

[122] Article 9 (2) (e) GDPR.
[123] See Hoofnagle, van der Sloot and Borgesius, n 76, 83.
[124] Article 9 (2) (g) GDPR. Such processing must be undertaken on the basis of Union or Member State law, must be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.
[125] Article 9 (2) (h) GDPR. Such processing must be undertaken on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Article 9 (3).
[126] Article 9 (4) GDPR.

The GDPR enshrines several exemptions and restrictions of data protection rules for public health purposes. The processing of sensitive data -including health data- is allowed for reasons of public interest in the area of 'public health'.

'Public health' refers to 'all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality'.[127] Article 35 of the EU Charter of Fundamental Rights (EUCFR) guarantees a 'right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices' and provides that 'a high level of human health protection shall be ensured in the definition and implementation of all the Union's policies and activities'.

More particularly, the GDPR permits the processing of health data when this is necessary to protect 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'.[128] The public interest in the area of public health does not have to be 'substantial',[129] and this provision provides a basis for the processing of health data without needing any other legal basis (such as the data subject's explicit consent).[130] The GDPR warns, however, that such processing of health data for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.[131]

[127] Regulation (EC) No 1338/2008 of the European Parliament and of the Council of 16 December 2008 on Community statistics on public health and health and safety at work, OJ L 354, 31.12.2008, p. 70. See also Recital 54 GDPR.
[128] Article 9 (2) (i) GDPR. Such processing must be undertaken on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.
[129] The European Data Protection Board (EDPD) seems to be requiring a 'substantial' public interest in this case too although this is not explicitly stated in Article 9 (2) (i) GDPR. See EDPD, Statement on the processing of personal data in the context of the COVID-19 outbreak, Adopted on 19 March 2020, 2.
[130] Article 9 (2) (i) GDPR requires that professional secrecy requirements, such as patient doctor confidentiality, should be respected in this case.
[131] Recital 54.

Recital 46 GDPR states that '[s]ome types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread'.[132] The current COVID-19 pandemic would be an example of such processing of personal health data that would be considered in the public interest in the area of public health and, therefore, permitted.[133]

The GDPR allows restrictions to data protection principles and data subjects' rights taken on the basis of 'public health' purposes.[134] Such restrictions can be imposed by EU or Member States' law by way of a 'legislative measure' that respects the essence of the fundamental rights and freedoms and is necessary and proportionate in a democratic society.[135] The GDPR also includes a 'public health' exemption to the right to erasure ('right to be forgotten') that obliges controllers to erase personal data concerning a data subject if requested to do so.[136] This means that if further retention of the personal data is necessary for public health reasons, the controller is not obliged to erase them even if the data subject has exercised her right to erasure. Furthermore, the GDPR provides a number of derogations from the general rule that personal data can be transferred to third countries outside the EU only when these provide an adequate level of protection[137] or appropriate safeguards, including binding corporate rules.[138] A case where such international transfer can take place without appropriate safeguards or an adequacy decision is when the transfer is 'necessary for important reasons of

[132] See also Recitals 45, 52 and 54.
[133] EDPD, n 129, 2.
[134] Article 23 (1) (e) GDPR. See also Recital 73.
[135] Ibid. According to Article 23 (2) GDPR such measures should 'contain specific provisions at least, where relevant, as to: (a) the purposes of the processing or categories of processing; (b) the categories of personal data; (c) the scope of the restrictions introduced; (d) the safeguards to prevent abuse or unlawful access or transfer; (e) the specification of the controller or categories of controllers; (f) the storage periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing; (g) the risks to the rights and freedoms of data subjects; and (h) the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.'
[136] Article 17 (3) (c) GDPR. See also Recital 65.
[137] Article 45 (3) GDPR.
[138] Article 46 GDPR.

public interest'[139] that include 'public health, for example in the case of contact tracing for contagious diseases'.[140] Such derogation could be used, for instance, to allow for the transfer of EU originating personal data to third countries that do not guarantee an adequate protection to combat the COVID-19 pandemic and trace the contacts' spread of this virus.

Finally, the GDPR makes clear that it applies to personal data processed for 'scientific research purposes', including technological development and demonstration, fundamental research, applied research and privately funded research.[141] According to the GDPR, 'scientific research purposes' also include studies conducted in the public interest in the area of public health.[142] If the result of scientific research in the health context gives reason for further measures in the interest of the data subject, the general rules of the GDPR are also applicable to those measures.[143]

3.5 Assessing the GDPR's health related legislative choices

Overall, it is clear that the GDPR's provisions examined above constitute a legislative attempt to *balance* two distinct forms of fundamental values and interests: those of data privacy and those of public health. Whether the GDPR achieves a fair balance in this respect, is a question that remains to be answered. However, a number of points can be raised in this regard.

First, the GDPR takes a clear position on the question 'for the benefit of whom' the balancing between the fundamental interests of data privacy and public health should be taking place. As Recital 53 puts it,

[139] Article 49 (1) (d) GDPR. See also Article 49 (1) (f) that allows the transfer if it 'is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent'.
[140] Recital 112 GDPR.
[141] Recital 159 GDPR. See also Article 179(1) TFEU.
[142] Ibid.

> Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes *for the benefit of natural persons and society as a whole...*[144]

This is a significant choice made by the EU legislator that provides the benchmark for the balancing exercise; this must always be undertaken for the benefit of individuals and the society as a whole.

Second, the question of balancing between data privacy interests, on the one hand, and public health interests, on the other hand, is a context-dependent one. These interests are prioritised differently depending on the context within which they arise: In situations -much like the current COVID-19 pandemic- where the monitoring of epidemics and their spread is required, public health interests are prioritised over data privacy. Under normal processing circumstances, data privacy interests are prioritised and the GDPR recognises increased levels of protection of 'health data' compared to normal sensitive data. There are exemptions, restrictions and exceptions under normal processing circumstances as well- these prioritise in particular cases, public health interests. In this respect, the GDPR has done a good job as it adopts a degree of flexibility when considering the different interests at stake.

Third, where public health restrictions are required these must be prescribed by law, be necessary in a democratic society, respect the principle of proportionality and be accompanied with appropriate (data protection) safeguards. Such safeguards are crucial and must be respected even in exceptional times, such as the ongoing coronavirus pandemic.[145]

What makes the GDPR's legislative choices more problematic, however, is their *binary* nature. This brings me to the fourth point I would like to make. The GDPR follows a 'black/white approach'[146] regarding health data privacy. The data are either sensitive or not; if

[144] Emphasis added.
[145] See EDPD, n 129, 1.
[146] Nikolaus Forgo, 'My health data—your research: some preliminary thoughts on different values in the General Data Protection Regulation' (2015) 5 (1) *International Data Privacy Law* 54, 59.

they are, then they enjoy increased protections. They are either personal or not- if they are, the data protection rules apply; if not, they fall altogether outside the scope of the GDPR. Such distinctions and dichotomies based on a binary approach are difficult to maintain in the big data analytics environment. They often make little sense and entail a risk of both regulatory over-inclusiveness and under-inclusiveness. Strict and rigid rules based might not be necessary at every instance; [147] conversely, the GDPR's rules and protections regarding health data might fall short in effectively protecting individual and societal interests in certain cases.

4. Conclusion

The COVID-19 pandemic has brought forward a plethora of challenges that data privacy faces both known and unknown.[148] Health surveillance, however, is hardly new. This has often taken place also outside the traditional healthcare context through a variety of mhealth apps, devices and social media platforms.

The GDPR contains a broad definition of data concerning health and recognises augmented protection to these as sensitive data. This illustrates that the EU legislator considers health data privacy as an important interest often at risk that merits additional protection. At the same time, the GDPR includes several exemptions and restrictions to health data privacy interests. Some of these are based on the individual circumstances of data subjects (e.g. 'explicit consent' or to protect the 'vital interests' of the data subject), but most of them concern public health interests.

[147] See for example Forgo that discusses medical research and argues that in certain cases this might produce (incidental) findings with relevance to the participants. 'In such cases it might be necessary for the physician as an investigator to re-identify the trial participant'. Ibid, 58.
[148] See for instance revelations that the UK government is sharing confidential National Health Service (NHS) patient data with private tech firms to build 'a COVID-19 datastore'. Paul Lewis, David Conn and David Pegg, 'UK government using confidential patient data in coronavirus response', *The Guardian*, 12 April 2020 < https://www.theguardian.com/world/2020/apr/12/uk-government-using-confidential-patient-data-in-coronavirus-response>.

The GDPR's provisions balancing data privacy with public health interests appear flexible and context- dependent. In this regard, data protection rules 'can in no manner be an obstacle to saving lives'[149] and 'do not hinder measures taken in the fight against the coronavirus pandemic'.[150] At the same time, exceptional measures should be adopted only when it is necessary and must be proportionate and followed by data privacy safeguards. This demonstrates that the GDPR enshrines the rule of law principle. Exceptional circumstances measures cannot appear and operate in a democracy vacuum; they must be taken in accordance with the rule of law and the principle of proportionality as they operate in a democratic society. This also confirms that the GDPR does not allow the exploitation of exceptional circumstances introduced to combat COVID-19 'to usher in an era of bio-surveillance' that will persist even after the pandemic has ended.[151]

While the GDPR can be applauded for striking a reasonably fair balance between data privacy and public health interests, the binary, black/white approach it adopts regarding sensitive (health)/ non-sensitive (non-health) is problematic. Such distinctions are difficult to make in a big data context using AI analytics and entail the risk of rendering the GDPR's rules both over- and under- inclusive.

[149] Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe, Strasbourg, 30 March 2020.
[150] EDPD, n 129,
[151] This was argued by Edward Snowden. See David Pegg and Paul Lewis, 'NHS coronavirus app: memo discussed giving ministers power to 'de-anonymise' users', *The Guardian*, 13 April 2020 < https://www.theguardian.com/world/2020/apr/13/nhs-coronavirus-app-memo-discussed-giving-ministers-power-to-de-anonymise-users> .