Chapter 10
Data Protection and Ethical Issues in European P5 eHealth

Virginia Sanchini and Luca Marelli

1 Introduction

In spite of its promise to significantly ameliorate health and care practices, the momentous rise of eHealth technologies—an umbrella term that refers to a varied set of tools and resources such as health information networks, electronic health records, telemedicine and monitoring services, wearable systems, as well as online health self-management tools—has been fraught with significant ethical and societal concerns. Thriving out of the extensive use of (sensitive) personal data (i.e., Big Data approach), while also representing a major driver for reconfiguring entrenched social practices and relations within health and care systems, eHealth has been the focus, in recent years, of increased ethical, legal, and sociological scrutiny.

Aimed at providing an overview of the data protection regime and the main ethical issues associated with the emergence and progressive stabilization of eHealth within the context of the European Union (EU), this chapter is structured as follows. First, innovation in eHealth as a core policy objective of the EU is presented; then, regulatory issues related to eHealth research and innovation are discussed; notably, our attention will be devoted to the discussion of eHealth technologies in light of the

The Authors Virginia Sanchini and Luca Marelli have contributed equally to this work.

V. Sanchini (✉)
Faculty of Philosophy, Università Vita-Salute San Raffaele, Milan, Italy

Department of Oncology and Hemato-Oncology, University of Milan, Milan, Italy
e-mail: sanchini.virginia@hsr.it; virginia.sanchini@unimi.it

L. Marelli
Life Sciences & Society Lab, Centre for Sociological Research, KU Leuven, Belgium

Department of Experimental Oncology, IEO, European Institute of Oncology IRCCS, Milan, Italy
e-mail: luca.marelli@kuleuven.be; luca.marelli@ieo.it

regulatory regime unfolding in Europe following the enforceability of the new legislation on data protection, Regulation (EU) 2016/679, also known as the General Data Protection Regulation. Finally, the second part of the chapter will provide an overview of the main ethical challenges raised by the development and implementation of novel eHealth technologies.

2   eHealth in the European Union: From Advancement of Innovation to Data Protection Concerns

Ever increasingly since the launch of the Lisbon Agenda at the turn of the millennium, the European Union (EU) has targeted the acceleration of scientific and technological innovation as a key policy objective. Emphasized as one of the privileged means to steer the EU out of its current economic and political gridlock, the acceleration of innovation has also been envisaged as a prominent lever to relaunch the promise of the European project and to promote the further consolidation of the fragile European polity (Marelli and Testa 2017).

Notably, innovation in eHealth, which thrives out of advances in fields such as personalized medicine, Artificial Intelligence, Big Data Analytics and mobile Health (mHealth) technologies, has emerged, in recent years, as a major recipient of knowledge and material investments from the part of the Union, geared to "strengthen[ing] the resilience and sustainability of Europe's health and care systems" and "maximiz[ing] the potential of the digital internal market with a wider deployment of digital products and services" (EC 2018: 4). Specifically, the latest Communication from the European Commission on *Enabling the digital transformation of health and care in the Digital Single Market* (EC 2018) has identified three key objectives to be accomplished through the full-fledged digitization of health and care systems and the (yet-to-be-achieved) completion of the Digital Single Market—a policy cornerstone of the European Commission under the presidency of Jean-Claude Juncker—in the health and care domains.

Firstly, the Commission set out its intention to enhance the sharing of health data across borders, by "supporting the development and adoption of a European electronic health record exchange format" (EC 2018, p. 5), predicated on the interoperability of standards across Member States, the development of EU-wide standards for data quality, reliability and cybersecurity, as well as potential (re)use of data for research and other purposes. A second envisaged objective is represented by the "pooling of genomic and other health data to advance research and personalized medicine" (EC 2018, p. 7). Specifically, against the backdrop of a flurry of initiatives having mushroomed throughout European Member States in recent years, the EU is tasked with "linking national and regional banks of -omics data, biobanks and other registries," with the aim of "provid[ing] access to at least 1 million sequenced genomes in the EU by 2022" (EC 2018, p. 8). Thirdly—and most relevantly for the purposes of this chapter—the digitization of health and care through

the integration of eHealth technologies and practices in health and care systems is framed as directed toward the enactment of "citizen empowerment and person-centered care" (EC 2018, p. 10). Indeed, ageing of the population together with the growing burden of chronic conditions and multi-morbidity are said to require profound changes in health and care systems (cf. Chap. 1). As contended by the Commission, what is required is, in particular, a "shift from treatment to health promotion and disease prevention, from focus to disease to a focus on well-being and individuals, and from service fragmentation to the integration and coordination of services along the continuum of care" (EC 2018, p. 10).

Notwithstanding the emphasis placed on the advancement of innovation in the eHealth sector, poised to the creation of a "Europe-wide ecosystem for data-driven healthcare" (Smith 2018), EU policymakers have been equally alerted to the privacy and data protection concerns European citizens maintain when confronted with these new technologies and practices (Mager 2017). Accordingly, following trilogue (and extensively lobbied) negotiations started in 2012, in 2016 the European Parliament has approved Regulation (EU) 2016/679 on data protection, also known as the General Data Protection Regulation (GDPR). As remarked by its rapporteur, German MEP Jan Albrecht, the GDPR is intended to provide "the right balance between the fundamental right to data protection as well as strong consumer rights in the digital age, on the one side, and the need to create a fair and functioning digital market, with a real chance for growth and innovation, on the other side" (Albrecht 2016).

In what follows, we will explore the impact of the GDPR on the European eHealth sector. In particular, our focus is directed at charting some of the key provisions of the GDPR that affect research and innovation processes in the eHealth sector. Besides, we will probe the implications of the Regulation as to the balancing of the interests and fundamental rights of individuals and the advancement of eHealth innovation.

3   The GDPR and Its Impact on eHealth Research and Innovation

The GDPR, which repeals the previous European legislation on data protection, Directive 95/46/EC, has become applicable since May 25, 2018. Differently from the previous Directive, which required adoption in national legislations, the GDPR is directly enforceable across all Member States, and is thus geared to achieve immediate and thorough legislative harmonization across the EU. Besides providing regulatory support for the establishment of a full-fledged digital single market, its entry into effect is bound to impact the eHealth sector very significantly, in the EU and possibly beyond. How, and to what effect, is what we aim to chart in the following sections.

At its core, as enshrined in the "data protection by design and by default" principle (art. 25), the GDPR adopts a risk-based approach to data protection, geared to ensure that appropriate data protection measures are designed and implemented throughout the entirety of the data processing activities. Additionally, it confers novel rights to data subjects, such as the right to data portability (art. 20) and the so-called right to be forgotten (art. 17). While the former bestows on individuals the right to require that data concerning them be standardized and made portable across companies or service providers of their choice, the latter empowers data subjects to obtain from data controllers the prompt erasure of relevant personal data. Moreover, the GDPR prescribes the adoption of specific provisions for the processing of sensitive data (art. 9) for scientific research purposes (art. 89), such as technical and organizational measures (e.g., pseudonymization), which are meant to provide adequate safeguards to the rights and freedoms of data subjects. Such provisions—which we will explore more in detail below—are poised to have a great impact on the development and commercialization of novel eHealth tools and technologies. Relevantly, the GDPR also endows Member States with the prerogative to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health (art. 9(4)).

3.1   The Accountability Principle and its Implications

In general terms, the axiomatic cornerstone of the GDPR can be said to be represented by the "accountability principle" (art. 5(2), art. 24), which requires data controllers (i.e., the persons, companies, associations, or other entities that are factually in control of personal-data processing) to adopt a proactive approach toward data protection compliance. Notably, data controllers are made responsible to assess, implement, and verify the adoption of appropriate technical and organizational measures to ensure, and be able to demonstrate, that data processing complies with the GDPR (art. 24). The GDPR itself provides coarse-grained guidance as to what measures actually fulfill a controller's obligations, and in fact makes the determination of those measures dependent on the contingent "nature, scope, context and purposes" of the relevant processing (art. 24). Accordingly, it can be argued that the GDPR is bound to promote a "controller-based," "case-sensitive," and eminently "context–specific" approach to data protection (Marelli and Testa 2018).

Such decentralized, flexible, and accountability-based approach rises to significance with respect to two aspects that are of key importance in the development and adoption phase of eHealth technologies, namely, consent and secondary use of data (further processing). With regard to consent, the GDPR requires the "specific [and] informed" consent of the data subject (art. 6(1)(a) and recital 32). However, when it comes to the processing of personal data within research—as can be the case in the developmental phase of eHealth technologies, such as mHealth apps, telemedical or Ambient Intelligence tools—it recognizes that it may not be possible to fully identify all potential future research purposes at the time of data collection. Accordingly,

as per recital 33, it states that, if too specific a consent would impinge on the purpose of research, "data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognized ethical standards for scientific research." Otherwise put, such provision lends the full legislative weight of the GDPR in support of broad consent, whenever the criterion of specific consent for specific research use at the moment of data collection proves impossible to satisfy (Marelli and Testa 2018).

As for the further use of previously collected and processed data—a key requirement for Big Data processing—article 5(1)(b) of the GDPR mandates that personal data should be "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes." Additionally, it specifies that further processing for scientific research purposes "shall […] not be considered to be incompatible with the initial purposes" for which personal data have been collected. More specifically, the GDPR requires controllers to carry out, on a case-by-case and context-dependent basis, a "test" for compatibility assessment, geared at ascertaining whether the further processing of personal data without data subject's consent is compatible with the initial purpose for which data were originally collected (art. 6(4)). Factors such as the "the reasonable expectations of data subjects based on their relationship with the controller as to their further use" (recital 50), and "the context in which the personal data have been collected," are among the key elements to be taken into account for assessing the compatibility of the intended further processing (art. 6(4)).

3.2   Pseudonymization and Anonymization of Sensitive Data

An important distinction introduced by the GDPR is the one between pseudonymized and anonymous data. Art. 4(5) defines "pseudonymization" as "*the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*" On the contrary, anonymous data are defined, as per recital 26, as "*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.*" This difference has significant implications. On the one hand, pseudonymized data—insofar as they can be attributed to the data subject through the use of "additional information"—are considered as personal data whose processing should comply with the GDPR. On the other hand, the provisions of the GDPR "do not concern the processing of anonymous information, including for statistical or research purposes" (recital 26). In other words, whereas the processing of pseudonymized information should be subjected to the full spectrum of provisions contained in the GDPR, individuals will not be entitled to data protection rights if their data are processed anonymously.

But what does constitute "anonymous" processing (or, better phrased, processing of "anonymous" data) in light of the GDPR? Interestingly, the GDPR differs conspicuously, in this respect, from other major data protection legislations world-wide, such as the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in the USA (Shabani et al. 2018). Within the Privacy Rule, the Safe Harbor standard for achieving the de-identification of personal data singles out 18 distinct identifiers, the removal of which is said to make the resulting information "not individually identifiable," and thus anonymous. Differently from this, recital 26 of the GDPR states that personal data should be considered anonymous insofar as the data subject cannot be identified "by any means reasonably likely to be used […] either by the controller or by any other person" (GDPR recital 26; see also Article 29 Working Party,18 opinion 05/2014). To ascertain whether means are reasonably likely to be used to identify the natural person, the GDPR further states that "account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments" (recital 26).

As such, and in line with the overall decentralized thrust of the Regulation, the GDPR can be said to adopt a context-based criterion to determine whether personal data should be considered as irreversibly de-identified (and thus anonymous), while devolving to controllers the responsibility to address such a question (is there a "reasonable likelihood" that reidentification techniques can be effectively used to de-anonymize my given dataset?) in the context of their concrete processing activities.

Moreover, the definition of "anonymous data" advanced by the GDPR seems to create a "catch-22" situation (Shabani and Marelli 2019). On the one hand, as we have seen, the processing of anonymous data is not subjected to the safeguards entailed by the GDPR, and this represents an implicit incentive to the processing and sharing of anonymous information. On the other hand, however, *precisely* the absence of said safeguards, as well as the enhanced circulation of data, are factors that, in themselves, are bound to *increase* the likelihood of reidentification of the data subject, which, in turn, can lead to the de-anonymization of the dataset. Thus, the very approach toward anonymous data processing adopted by the GDPR can be said to set a high legal bar for achieving anonymization of data (Quinn and Quinn 2018)—especially in the context of the processing of genetic data (Shabani and Marelli 2019).

3.3 The "Right Balance" Between Innovation and Protection of Individuals' Rights and Interests?

As explicitly stated in the Regulation, the adoption of the GDPR has been underpinned by the aim to accomplish, at once, two seemingly contrasting objectives, namely, the protection of the fundamental rights and freedoms of individuals with regard to the processing of personal data (i.e., data protection), and the enhancement

of the free movement of personal data within the EU, in view of the creation of a full-fledged Digital Single Market poised to foster digital innovation (i.e., data utility). For such "data protection–versus–data utility" conundrum, the implementation of a controller-based and decentralized approach to data protection, in place of rigid and detailed provisions, can be assessed ambivalently.

On the one hand, beside the introduction of novel rights for data subjects, the flexibility entailed by mechanisms such as the "compatibility test," as well as the enhanced role assigned to institutionalized ethics in defining the scope of data processing in Research & Innovation programs (on this aspect, cf. Marelli and Testa 2018), could be said to increase data subjects' protection while affording patients and/or research participants a substantive rather than mere formalistic engagement in the development and use of novel eHealth technologies.

On the other hand, however, in addition to the controllers' discretionary prerogatives, the GDPR upholds a far-reaching "research exemption" to the strict limitations otherwise imposed on the processing of sensitive data (art. 9(1)), for instance relaxing requirements for consent (recital 33) and limitations in data storage (art. 5(1)(e)). In addition, as per recital 159, the GDPR provides a remarkably broad definition of activities falling under the rubric of "scientific research," including "technological development and demonstration," "applied research," and "privately funded research." As a consequence, eHealth and mHealth companies (such as app providers, telemedical companies, AI companies, etc.), claiming to conduct "scientific research" activities with data gathered from individuals, stand to benefit directly from the regulatory leeway deriving from these combined provisions—with an arguably significant shift of the balance of interests in favor of data controllers over data subjects (Pormeister 2017; Marelli and Testa 2018).

In the final analysis, whether the GDPR will achieve the stated aim of ensuring the "right balance" between providing appropriate safeguards to individuals—thus allaying still widespread privacy and data protection concerns surrounding eHealth technologies (Powles and Hodson 2017)—and creating the conditions for a thriving Digital Single Market in domains such as health and care, is something that only its implementation in the coming months and years will be able to tell.

4 Ethical Issues in eHealth Technologies

Notwithstanding the similar data protection concerns raised, the expression "eHealth" (cf. Eysenbach 2001) connotes a vast array of different technologies (as well as their related social practices), each of which raises distinct ethical issues. In what follows, eHealth technologies will be divided into three broad families:

- Online eHealth (self-management tools)
- Monitoring techniques
- New and unconventional eHealth technologies

The respective ethical aspects will be discussed separately.

4.1 Online eHealth (Self-Management) Tools

One of the most widespread forms of eHealth is represented by consumers' demand for online health information, which remains "one of the most important subjects that internet users research online" (Fox 2011a). Besides dedicated websites, health-related information is increasingly being accessed through blogs and social media. According to Fox, the information most commonly searched for within this broad category is that referring to diseases and/or medical problems, medical treatment and/or medical procedure, or information regarding doctors or other health-care professionals (Fox 2011a). The same study has also shown that the vast majority of online eHealth consumers consists of people affected by chronic diseases, whose primary aim is not only that of broadening the information at their disposal but also finding "peers," that is, people affected by their same condition, with whom they can share their experiences and from whom they could receive advice and/or support.[1] Giving rise to distinct forms of "biosociality" (a term coined by renowned anthropologist Paul Rabinow (1996) to capture the emergence of new collectivities, social networks, and social interactions forming around shared biological—especially genetic—and medical characteristics), the so-called peer-to-peer health care (cf. Chap. 3) is rapidly expanding, in the USA and beyond (Fox 2011b).

By helping acquiring information with respect to health and health-related issues, eHealth technologies are said to provide individuals—independently of their literacy and/or economic status—with the opportunity "to become more informed and thus better prepared to discuss treatment plans with their physicians" (Czaja et al. 2013, p. 31; Taha et al. 2009). In particular, by facilitating peer-to-peer interactions and by allowing patients to get in touch with medical expert networks and/or patient associations, online eHealth technologies contribute to patients' acquaintance with health-related issues, thus promoting their improvement of medical literacy.

What has been just depicted as an emancipatory affordance of online eHealth tools may, however, give rise to a number of pitfalls. Firstly, the much too informed online individual may become a distrustful patient, unwilling to adhere to medical advices provided in conventional face-to-face settings (Czaja et al. 2013). Secondly, such individual may equally turn into a consumer of online commercialized products lacking clear medical or preventive benefits without adequate medical oversight—something that has been shown to occur, for instance, in the case of unproven stem cell therapies as well as Direct-to-Consumer genetic tests (cf., e.g., Wallace 2011).

Another criticality ascribed to online eHealth self-management tools concerns the way in which online eHealth information is presented and its tools are designed.

---

[1] Other sets of people who are likely to engage in online searches for people sharing their same health concerns include "internet users who are caring for a loved one; internet users who experienced a medical crisis in the past year; and internet users who have experienced a significant change in their physical health, such as weight loss or gain, pregnancy, or quitting smoking" (Fox, 2011b).

Indeed, despite its promise of improving access to health information, "to date many Internet-based health applications have been designed without consideration for needs, capabilities, and preferences of user group[s]" (Czaja et al. 2013, p. 31). Although it should be recalled that the group of users looking for health information online is rather heterogeneous—spanning from adults to older adults, affected by chronic as well as nonchronic conditions—these tools and platforms are often devised without considering the potential difficulties that users may encounter in navigating this information and understanding its content.

To summarize, two main sets of criticalities may be ascribed to eHealth online technologies: while the former—distrust toward medical experts, patients-turned-consumers without adequate medical oversight—represents a potential negative impact of the aforementioned technologies on online consumers, the latter—inadequacy of eHealth online tools with respect to target users—questions the appropriateness of technologies themselves to comply with the expectations set forth by their deployment.

A fruitful strategy for partially overcoming such issues may be found in the notion of *patient engagement* (cf. Chap. 1), defined as the act of involving patients—as well as the latter's availability of being involved—in their health and care processes (Gruman et al. 2010; Hibbard and Mahoney 2010; Clancy 2011; Barello et al. 2012; Menichetti et al. 2016). In broad terms, engaging patients has been considered as a key priority for contemporary health care and a policy objective in many countries (Thompson 2007). Besides fostering patients' capacity to significantly impact on the orientation, management, and evaluation of research programs concerning their diseases, "patient activation" has been associated with better adherence to treatments and improved treatment outcomes (Greene and Hibbard 2012; Vahdat et al. 2014).

In the context of the eHealth technologies under investigation here, patient engagement may lead to the design of technologies that more closely match users' preferences. Indeed, patients have been shown to adopt new technologies "if the tools are felt to be relevant to their own health-care problems, are engaging and easy to use, and are effective at achieving behaviour change" (Birnbaum et al. 2015, p. 754). As such, "without considering the patient as an active agent in the health-care environment," eHealth solutions run the risk "to be substantially ineffective in the end" (Triberti and Barello 2016, p. 151). As a consequence, "user-centered design" has been advanced as the "gold standard" for developing the eHealth tools of the future (cf. Chap. 9).

In addition, an engaged role from the part of the patients from the very onset of technological development can also reduce the risk that perceived harm related to technology usage (e.g., uncertainty about privacy rights, or about the management of one's own health data) would negatively influence users' acceptance at a later time. Indeed, despite the initial enthusiasm for eHealth technologies, some evidence exists that patients remain skeptical toward technological tools if these do not evolve

in line with their changes, renewed attitudes, and needs (Currie et al. 2015; Gaul and Ziefle 2009).[2]

4.2   Monitoring Techniques

A second family of eHealth technologies is the so-called monitoring techniques, that is, the set of techniques allowing a continuous observation of one's own condition (physiological and physical) performed through body and/or home sensors. Monitoring techniques were originally developed for improving health care locally, in those contexts in which geographical distances would have precluded regular health measures. Additionally, they have been typically devised for monitoring the behavior of chronic patients and/or the elderly, while communicating relevant health and/or behavioral information in real time to health-care professionals and/or their reference family member. Amongst the broad set of monitoring techniques, an important difference exists between more conventional monitoring techniques, such as telemedicine, and rather new and unconventional monitoring techniques, such as those labeled under the rubric of "Ambient Intelligence." These two sets of monitoring systems differ profoundly not only in terms of their technological capacities and impact on patients' health, but also in terms of ethical threats potentially related to their (ab)use.

Telemedicine, which literally means "healing at a distance" (Strehle and Shabde 2006), has been defined by the World Health Organization (WHO) as "the delivery of health-care services, where distance is a critical factor, by all health-care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities" (WHO 1998). According to this definition, telemedicine comprises sets of techniques aimed at overcoming the obstacles that may arise in providing assistance and/or care to a patient, using advanced telecommunication devices able to transmit medical information from the patient herself to the healthcare facility and vice versa, thus actively contributing to the improvement of health-care services. Despite their differences, the WHO has suggested to include, under the label "telemedicine," all those interventions (i) whose aim is to provide clinical support; (ii) which are intended to overcome geographical barriers, connecting users who are not in the same physical location; (iii) which involve the use of various types of information and communication technologies; (iv) whose broad goal is to improve health

---

[2] Actually, it is noteworthy to point out that the patient who let herself be engaged is neither a representative nor an average patient, but she is clearly a more active individual, with a better access to health care. Social determinants of health such as income, housing, social environments, and education have a real impact not only on health outcomes, but also on the opportunity to become a fully engaged patient.

outcomes (Ryu 2012, p. 9). Telemedicine applications are further classified in "store-and-forward" (or "asynchronous") interventions, in those instances in which telemedicine involves the exchange of prerecorded data between two or more individuals at different times, and "real time" (or "synchronous") interventions, when the involved individuals are simultaneously present for immediate exchange of information, as in the case of videoconferencing. Moreover, the interaction between the individuals involved may occur in the form of exchange between health-care professional and patient ("health professional-to-patient"), or between two or more health-care professionals ("health professional-to-health professional") (Ryu 2012, p. 10).

Traditional eHealth monitoring systems such as telemedicine in its different instantiations present several sets of advantages, among which the following are also ethically relevant. *Firstly* (cf. Chap. 4), they may improve health outcomes and allow patients to be assisted and/or cured in their home environments, while also reducing costs and inconveniences for patients due to prolonged admissions and hospital-based commuting. *Additionally*, they may enable the provision of high-quality home services, while prolonging as much as possible patients' independence—thus positively impacting on patients' quality of life. *Thirdly*, eHealth monitoring systems hold potential for improving health-care professionals' daily activities. Indeed, telemedicine is able to make available to the attending physician all the existing information related to the single patient and to send it, for consulting purposes, to specialists from all over the world; moreover, it contributes to reduce unnecessary administrative work, while at the same time enabling a more secure and organized management of information. *Finally*, by reducing prolonged and/or unnecessary hospitalizations, eHealth monitoring systems can also increase the efficiency and productivity of health services (Bauer 2001; Stanberry 2006). Monitoring technologies can therefore enable progress in the management and care of the chronic patient as well as of the elderly—leading to the identification of potential health problems before they become serious (cf. Chap. 5).

However, despite providing high data quality that may help ensure correct processing and interpretation of information, as well as the appropriate intervention of medical services, serious ethical concerns exist with respect to potential misuse of patients' information. In particular, the use of these technologies is usually accompanied with concerns related to *informational privacy*, that is, regarding what type of information is recorded, how it is recorded, and with whom it is shared. This appears particularly controversial in case of new and unconventional aforementioned monitoring systems, such as Ambient Intelligence.

Ambient Intelligence refers to the sets of different physical environments—such as homes, offices, meeting rooms, schools, hospitals, control centers, vehicles, tourist attractions, stores, and sports facilities (Ramos et al. 2008)—that "intelligently and unobtrusively" interact with people, through a "world of ubiquitous computing devices" (Ramos et al. 2008, p. 15), such as micro-computers and different types of sensors, in order to systematically monitor the daily activities of the target users. Despite referring to different kinds of environments, Ambient Intelligence has been bound, in recent literature (Ramos et al. 2008; Cook et al. 2009; Acampora et al.

2013), to the presence of some distinctive features: "it is context aware (it makes use of information drawn on the here-and-now situation); personalized (it is tailored on the individual user's needs); anticipatory (it develops the capacity of predicting user's needs); adaptive (it is able to modify its own functions/behavior on the basis of the user's habits); ubiquitous (it is embedded and distributed among the environment); transparent (it is able to function without direct action, nor perception, nor knowledge by the human user)" (Triberti and Barello 2016, p. 151).

As embedded in environments structurally and inherently devised to monitor human behavior, Ambient Intelligence raises at least three kinds of ethical concerns with respect to the target user that need to be considered and properly handled.

- *Firstly*, and as already mentioned, the most relevant ethical concern regards informational privacy. In the case of Ambient Intelligence, as some scholars have noticed, almost any kind of data gathering may potentially represent a privacy violation. As an example, the use of image processing through video cameras as a potential kind of sensor has been deemed "a controversial area" (Cook et al. 2009, p. 287), as cameras filming users in specific conditions and/or while performing certain activities may appear as a violation of the individual personal sphere. In line with this observation, it is interesting to notice that, according to empirical evidence collected (Beach et al. 2009, 2010), requests for greater confidentiality exist with respect to information acquired in certain specific house areas (such as the bathroom and bedroom) where privacy violation is intuitively perceived as more serious by the side of the target user. Besides implementation of the GDPR's accountability-based approach described in the first part of this chapter, solutions exist in order to limit privacy concerns, such as limiting cameras registration to specific environments and in space obscuring bodies, but, as it has been pointed out, even seemingly innocuous ones such as walking patterns and eating habits can be combined to provide very detailed information on a person's identify and lifestyle (Bohn et al. 2005).
- *Secondly*, and relatedly, the so-called big brother syndrome (Dwight and Feigelson 2000), that is, the negative feeling of being observed by the technology itself, may have an impact on personal behavior, inasmuch as individuals may modify their behaviors precisely as a consequence of knowing of being registered, thus limiting *de facto* their personal liberties. Ambient Intelligence technologies, in this respect, may shape individual behaviors, leading to the self-disciplining of the individual.
- *Finally*, concerns related to the actual validity of users' authorization toward these techniques have been raised. Indeed, despite the rhetoric of transparency with respect to Ambient Intelligence systems, several doubts exist with respect to the validity of target users' consent, as the latter may be based on user's misconceptions and/or partial misrepresentation of the system and its functioning, based upon preliminary explanations that may hardly convene adequate representations of the system in which the user will be embedded. In addition to enriching the oral explanation of Ambient Intelligence systems with videos and figurative representations, a possible solution may be that of envisaging a "multistep

consent" to be provided at different time points, not only before, but also in between distinct set up phases of the system.

4.3   New and Unconventional eHealth Technologies

In addition to the aforementioned and more conventional eHealth technologies, a set of novel and less conventional eHealth technologies has recently emerged and/ or developed in the health and medical domains, raising distinct sets of ethical issues.

Artificial Intelligence. A first domain in which eHealth technologies are rapidly evolving revolves around the adoption of Artificial Intelligence (AI) within the medical context and, in particular, as a clinical care tool. Inasmuch as some areas of medicine, such as radiology, pathology, and dermatology, find themselves dealing with increasing amount of data, they are likely to adopt AI tools, in order to "extract fine information about issues invisible to the human eye and process those data quickly and accurately" (Jha and Topol 2016). In this context, such emerging technology may run the risk of impacting on the epistemic and social authority of physicians and medical specialists. At the same time, however, the idea that the AI will inevitably displace medical expertise and reconfigure entrenched epistemic and social relations between doctors and patients seems largely far-fetched. As analysts have noted, "given that artificial intelligence has a 50-year history of promising to revolutionize medicine and failing to do so, it is important to avoid overinterpreting these new results" (Beam and Kohane 2016, p. E2).

Virtual Reality. Virtual reality (or environment) is defined as a "spatial (usually 3D) world seen from a first person's point of view" where the view "is under the real-time control of the user" (Lányi 2006, 87). In recent years, virtual reality has rapidly emerged as a promising technology in the health-care domain, in particular in diverse sensitive settings such as aged care, clinical rehabilitation, and mental health (Valmaggia et al. 2016; Moyle et al. 2017). With regard to this latter domain, some scholars have recently observed that, because of its power to simulate the environmental conditions that trigger problems, it may be used to treat phobias, posttraumatic stress disorders, and to induce empathy and other altruistic-based behaviors in patients (Freeman et al. 2017). Moreover, inasmuch as it is an immersive technology, virtual reality has the potential to be introduced effectively in pain management, distracting chronic patients from their experience of pain (Gromala et al. 2015). In addition to some practical challenges in implementing virtual reality technologies, for example, the costs of implementation and the need for one-on-one assistance from care staff (Waycott et al. 2018), some ethical challenges may also arise. First, due to the novelty of the technology itself, possible system failures may happen, which may be interpreted by vulnerable participants as signs of failure on their part (Waycott et al. 2018, p. 412). Secondly, and more importantly, inasmuch as virtual reality involves

being immersed in an alternate reality, it may amplify people's experience, creating experiences of confusions and even trauma, which may be particularly problematic for those vulnerable categories of individuals for which these techniques are deployed (Vines et al. 2017).

Virtual Worlds. A further development of virtual reality is represented by virtual worlds, consisting of technologies devised so as to provide users with the possibility to share the experience of an interactive virtual environment through the creation, customization, and use of avatars (Morie and Chance 2011), thus combining the advantages of virtual realities environments with the connectivity offered by social networks. Despite their potential impressive impact in health care, particularly as tools promoting a high level of education for health-care professionals, some doubts have been raised with respect to the involvement of patients in these settings. Indeed, inasmuch as the virtual worlds are contexts where different individuals are simultaneously present, it is not always possible to predict the (ab)use and the impact these systems will have on patients themselves (Triberti and Chirico 2017).

5 Conclusions

This contribution has explored the regulatory landscape that, after the entry into effect of the GDPR, underpins the unfolding of eHealth research and innovation in the EU. As we have observed in the chapter, the GDPR promotes a decentralized approach to data protection—centered on the accountability of data controllers. Whether this approach will be effective in achieving an effective balance between protection of the rights and interests of individuals (data subjects) and the promotion of innovation in the eHealth sector is, at the time of writing, still a major open question.

Moreover, this contribution has provided an overview of the societal and ethical challenges raised by the development of novel digital technologies, examining some important ethical issues that may arise when developing and implementing eHealth solutions for health management in the context of medical (e.g., chronic) conditions. In conclusion, we stress that, regarding the psycho-cognitive factors in P5 eHealth technologies, it is still paramount to develop a set of psychometric instruments able to capture the important psychological characteristics that would allow (1) the user (patient)-centered design of devices and interfaces, in order to tailor eHealth solutions on users' needs, and (2) the adequate technology-mediated analysis of patients' characteristics to be considered within the field of chronic illness management.

References

Acampora, G., Cook, D. J., Rashidi, P., & Vasilakos, A. V. (2013). A survey on ambient intelligence in healthcare. *Proceedings of the IEEE, 101*(12), 2470–2494.

Albrecht, J. (2016). *Conclusion of the EU data protection reform*. Available at: https://www.janalbrecht.eu/2016/04/2016-04-13-conclusion-of-the-eu-data-protection-reform/

Barello, S., Graffigna, G., & Vegni, E. (2012). Patient engagement as an emerging challenge for healthcare services: mapping the literature. *Nursing Research and Practice, 2012*.

Bauer, K. A. (2001). Home-based telemedicine: A survey of ethical issues. *Cambridge Quarterly of Healthcare Ethics, 10*(2), 137–146.

Beach, S., Schulz, R., Downs, J., Matthews, J., Seelman, K., Barron, B., & Mecca, L. (2009, October). End-user perspectives on privacy and other trade-offs in acceptance of quality of life Technology. In *Gerontologist* (Vol. 49, pp. 164–164).

Beach, S., Schulz, R., Downs, J., Matthews, J., Seelman, K., Person Mecca, L., & Courtney, K. (2010). Monitoring and privacy issues in quality of life technology applications. *Gerontechnology, 9*(2), 78–79.

Beam, A. L., & Kohane, I. S. (2016). Translating artificial intelligence into clinical care. *Jama, 316*(22), 2368–2369.

Birnbaum, F., Lewis, D., Rosen, R. K., & Ranney, M. L. (2015). Patient engagement and the design of digital health. *Academic Emergency Medicine, 22*(6), 754–756.

Bohn, J., Coroamă, V., Langheinrich, M., Mattern, F., & Rohs, M. (2005). Social, economic, and ethical implications of ambient intelligence and ubiquitous computing. In *Ambient intelligence* (pp. 5-29). Springer, Berlin, Heidelberg.

Clancy, C. M. (2011). Patient engagement in health care. *Health Services Research, 46*(2), 389–393.

Cook, D. J., Augusto, J. C., & Jakkula, V. R. (2009). Ambient intelligence: Technologies, applications, and opportunities. *Pervasive and Mobile Computing, 5*(4), 277–298.

Currie, M., Philip, L. J., & Roberts, A. (2015). Attitudes towards the use and acceptance of eHealth technologies: A case study of older adults living with chronic pain and implications for rural healthcare. *BMC Health Services Research, 15*(1), 162.

Czaja, S., Beach, S., Charness, N., & Schulz, R. (2013). Older adults and the adoption of healthcare technology: Opportunities and challenges. In *Technologies for active aging* (pp. 27-46), Boston, MA: Springer.

Dwight, S. A., & Feigelson, M. E. (2000). A quantitative review of the effect of computerized testing on the measurement of social desirability. *Educational and Psychological Measurement, 60*(3), 340–360.

EC. (2018). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018)33.

Eysenbach, G. (2001). Journal of Medical Internet Research is now indexed in Medline. *Journal of Medical Internet Research, 3*(3), e25.

Fox, S. (2011a). Health topics. Pew internet and American life project February 1, 2011.

Fox, S. (2011b). *Peer-to-peer healthcare*. Pew Internet & American Life Project.

Freeman, D., Reeve, S., Robinson, A., Ehlers, A., Clark, D., Spanlang, B., & Slater, M. (2017). Virtual reality in the assessment, understanding, and treatment of mental health disorders. *Psychological Medicine, 47*(14), 2393–2400.

Gaul, S., & Ziefle, M. (2009, November). Smart home technologies: Insights into generation-specific acceptance motives. In *Symposium of the Austrian HCI and Usability Engineering Group* (pp. 312–332). Springer, Berlin, Heidelberg.

Greene, J., & Hibbard, J. H. (2012). Why does patient activation matter? An examination of the relationships between patient activation and health-related outcomes. *Journal of General Internal Medicine, 27*(5), 520–526.

Gromala, D., Tong, X., Choo, A., Karamnejad, M., & Shaw, C. D. (2015, April). The virtual meditative walk: virtual reality therapy for chronic pain management. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 521-524). ACM.

Gruman, J., Rovner, M. H., French, M. E., Jeffress, D., Sofaer, S., Shaller, D., & Prager, D. J. (2010). From patient education to patient engagement: implications for the field of patient education. *Patient Education and Counseling, 78*(3), 350–356.

Hibbard, J. H., & Mahoney, E. (2010). Toward a theory of patient and consumer activation. *Patient Education and Counseling, 78*(3), 377–381.

Jha, S., & Topol, E. J. (2016). Adapting to artificial intelligence: radiologists and pathologists as information specialists. *Jama, 316*(22), 2353–2354.

Lányi, C. S. (2006). *Virtual reality in healthcare* (In *Intelligent paradigms for assistive and preventive healthcare* (pp. 87-116)). Berlin, Heidelberg: Springer.

Mager, A. (2017). Search engine imaginary: Visions and values in the co-production of search technology and Europe. *Social Studies of Science, 47*(2), 240–262.

Marelli, L., & Testa, G. (2017). *"Having a Structuring Effect on Europe": The Innovative Medicines Initiative and the Construction of the European Health Bioeconomy* (In *Bioeconomies* (pp. 73-101)). Cham: Palgrave Macmillan.

Marelli, L., & Testa, G. (2018). Scrutinizing the EU General Data Protection Regulation. *Science, 360*(6388), 496–498.

Menichetti, J., Libreri, C., Lozza, E., & Graffigna, G. (2016). Giving patients a starring role in their own care: a bibliometric analysis of the on-going literature debate. *Health Expectations, 19*(3), 516–526.

Morie, J. F., & Chance, E. (2011). Extending the reach of health care for obesity and diabetes using virtual worlds.

Moyle, W., Jones, C., Dwan, T., & Petrovich, T. (2017). Effectiveness of a virtual reality forest on people with dementia: A mixed methods pilot study. *The Gerontologist, 58*(3), 478–487.

Pormeister, K. (2017). Genetic data and the research exemption: is the GDPR going too far?.. *International Data Privacy Law*.

Powles, J., & Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. *Health and technology, 7*(4), 351–367.

Quinn, P., & Quinn, L. (2018). Big genetic data and its big data protection challenges. *Computer Law & Security Review, 34*(5), 1000–1018.

Ramos, C., Augusto, J. C., & Shapiro, D. (2008). Ambient intelligence—the next step for artificial intelligence. *IEEE Intelligent Systems, 23*(2), 15–18.

Regulation (EU). (2016/679). General Data Protection Regulation 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, which repeals Directive 95/46/ EC.

Ryu, S. (2012). Telemedicine: Opportunities and developments in member states: Report on the second global survey on ehealth 2009 (global observatory for ehealth series, volume 2). *Healthcare Informatics Research, 18*(2), 153–155.

Shabani, M., & Marelli, L. (2019). Re-identifiability of genomic data and the GDPR. *EMBO Reports*, e48316.

Shabani, M., Dyke, S. O., Marelli, L., & Borry, P. (2018). Variant data sharing by clinical laboratories through public databases: consent, privacy and further contact for research policies. *Genetics in Medicine, 1*.

Smith, H. (2018). *Data driven healthcare: Europe to change gear*. Available at: http://www.project-pulse.eu/data-driven-healthcare-europe-to-change-gear/

Stanberry, B. (2006). Legal and ethical aspects of telemedicine. *Journal of Telemedicine and Telecare, 12*(4), 166–175.

Strehle, E. M., & Shabde, N. (2006). One hundred years of telemedicine: does this new technology have a place in paediatrics? *Arch Disease in Childhood, 91*(12), 956–959.

Taha, J., Sharit, J., & Czaja, S. (2009). Use of and satisfaction with sources of health information among older Internet users and nonusers. *The Gerontologist, 49*(5), 663–673.

Thompson, A. G. (2007). The meaning of patient involvement and participation in health care consultations: a taxonomy. *Social Science and Medicine, 64*(6), 1297–1310.

Triberti, S., & Barello, S. (2016). The quest for engaging AmI: Patient engagement and experience design tools to promote effective assisted living. *Journal of Biomedical Informatics, 63*, 150–156.

Triberti, S., & Chirico, A. (2017). Healthy avatars, healthy people: care engagement through the shared experience of virtual worlds. In *Transformative healthcare practice through patient engagement* (pp. 247–275). IGI Global.

Vahdat, S., Hamzehgardeshi, L., Hessam, S., & Hamzehgardeshi, Z. (2014). Patient involvement in health care decision making: A review. *Iranian Red Crescent Medical Journal, 16*(1).

Valmaggia, L. R., Latif, L., Kempton, M. J., & Rus-Calafell, M. (2016). Virtual reality in the psychological treatment for mental health problems: An systematic review of recent evidence. *Psychiatry Research, 236*, 189–195.

Vines, J., McNaney, R., Holden, A., Poliakov, I., Wright, P., & Olivier, P. (2017). Our year with the glass: Expectations, letdowns and ethical dilemmas of technology trials with vulnerable people. *Interacting with Computers, 29*(1), 27–44.

Wallace, H. (2011). DTC Genetic Testing: A UK Perspective, GeneWatch Report 2011. Available at [Last accessed: 5 November 2018]: http://www.councilforresponsiblegenetics.org/gene-watch/GeneWatchPage.aspx?pageId=281&archive=yes

Waycott, J., Wadley, G., Baker, S., Ferdous, H. S., Hoang, T., Gerling, K., … & Simeone, A. L. (2018, May). Manipulating Reality?: Designing and Deploying Virtual Reality in Sensitive Settings. In *Proceedings of the 19th International ACM SIGACCESS Conference on Computers and Accessibility* (pp. 411–414). ACM.

WHO. (1998). A health telematics policy in support of WHO's Health-For-All strategy for global health development: Report of the WHO group consultation on health telematics, 11–16 December, Geneva, 1997. Geneva, World Health Organization.