eISSN 2783-6851

VILNIUS TECH
Vilnius Gediminas Technical University

NEW TRENDS in COMPUTER SCIENCES

2023
Volume 1
Issue 2
Pages 70–96
https://doi.org/10.3846/ntcs.2023.19166

EVOLUTION OF REGULATORY MODELS FOR PUBLIC HEALTH DATA ECOSYSTEMS FROM A LINKED DEMOCRACY PERSPECTIVE

Izabella LOKSHINA [1]✉, Cees LANTING[2]

[1]*Department of Business, State University of New York at Oneonta, Oneonta, USA*
[2]*DATSA Belgium, Consulting, Leuven, Belgium*

Article History:
- received 15 May 2023
- accepted 28 July 2023

Abstract. Public healthcare is a data-intensive environment that manages ever-increasing volumes of biomedical data resulting from medical data-generating technologies. In this paper, the authors discuss strategies to regulate the collection and use of biomedical data and metadata to build sustainable public health data ecosystems; this can assist citizens to get control of dataflows by defining identity in the public domain and shaping the capacity to use the web of data: get access to healthcare services and receive benefits and appropriate care. The authors suggest that a strategy based on the linked democracy governance model and safeguards, implemented through the meta-rule of law, enables better design of regulatory tools to handle semantically driven data flows. This strategy ties well in with models of deliberative and epistemic democracy, focused on relationships between people, data, and institutions. The authors investigate privacy, security, and data protection issues, applying existing ethical and legal frameworks for public health data and the theory of justice; they discuss the implementation of strategies to articulate the public domain and propose intermediate, anchoring institutions at the meso-level by building ontologies, selecting technical functionalities and algorithms, and embedding protections of the rule of law into specific public health data ecosystems.

Keywords: public health data ecosystems, linked democracy governance model, privacy, data protection, meta-rule of law, web of data, Electronic Health Record (EHR), identity.

✉Corresponding author. E-mail: ***izabella.lokshina@oneonta.edu***

Introduction

Ever-advancing medical technologies generating data, and the increased affinity towards data in general and associated analytics, provide unprecedented opportunities for patients and many other stakeholders in public healthcare that anyway has always been a data-intensive environment. These opportunities include the discovery of trends in public health, diagnosis and treatment of diseases, patient care, and public policy design, among others, by the use of, among others, Big Data, analytics, and Digital Twin approaches. At the same time, processes and generation, analysis, and combination of large datasets raise new challenges, including how to build data-intensive ecosystems that effectively address the needs of multiple stakeholders. Which methods, tools, standards, strategies, and regulatory instruments are required to make supportive ecosystems effective, efficient, sustainable, and still compliant with different legal and ethical frameworks?

This paper analyzes the application to public health data of a proposed regulatory framework for data-intensive ecosystems, an integral part of information and communications

technology (ICT). Like many other widely adopted technologies, ICT has become practically part of and greatly intertwined with society. This growing penetration of ICT in society along with wide-ranging application domains has resulted in citizens' awareness of dependencies and side effects, eventually leading to some form of governance for ICT, including legislation, regulation, standardization, and recommended practices. COVID-19 measures and related ICT applications, alongside other comprehensive applications, increasingly developing now under the term "artificial intelligence" (AI), have even further accelerated this process.

Therefore, the main research questions addressed by the authors in their investigation are as follows. First, given that some form of governance for ICT is necessary and needs to be developed, what would be the scope, priorities, and requirements for a suitable regulatory framework? Second, are there existing governance frames that can fulfill such requirements; or else, what could be the basis of a suitable regulatory framework to be developed? Third, what would the application of such a regulatory framework considered suitable for ICT look like?

As regards the first research question – based on preliminary studies, the authors identified the governance issues concerning data-intensive ecosystems as a priority, including such issues as data privacy, security, ownership, accountability, manipulation of complex and/or large volumes of data, data analytics, and complex decision processes; thereby also covering a significant part of AI applications and platforms.

As regards the second research question – despite some publications reviewing regulatory issues concerning data-intensive applications and platforms, the authors consider that the governance of data-intensive ecosystems received limited attention and has not been sufficiently covered. In fact, some publications have focused solely on the role of governance in either developing decentralized and data-intensive applications for the Internet of Things (IoT) or managing Big Data in a decentralized fashion. Other studies have concentrated mainly on data security, privacy, or ownership issues and the potential to enable trust and decentralization in either service ecosystems including public healthcare or data-intensive applications and platforms. Additional investigations have reflected mainly on either technical issues of data-intensive applications and platforms like existing protocols and vulnerabilities or technical characteristics of existing systems including usability, scalability, and data integrity, or else studied the governance of public health data only in conjunction with offered security and privacy. The literature lacks publications analyzing the governance of data-intensive environments including public health data ecosystems inclusively and comprehensively, a consideration that prompted this research and motivated authors to write this paper.

Accordingly, this paper is focused on the third research question – the authors evaluate the application of a linked democracy regulatory framework to public health data with safeguards implemented through meta-rule of law that can enable better design of the governance models required to handle semantically driven data flows, including Big Data. Additionally, the authors investigate the connection with deliberative and epistemic democracy regulatory models focused on relationships between people, data, and institutions, where the meta-rule of law constitutes an analytical extension of the rule of law with the use of semantic languages. Lastly, the authors discuss the implementation of privacy, security, and data protection strategies in public health data ecosystems to shape the public health data domain with a new institutional framework covering ethical foundations for these strategies.

This paper differs from the existing publications and contributes to the literature in two ways. First, the authors provide a comprehensive analysis of privacy, security, and data protection issues, applying existing ethical and legal frameworks for public health data and the theory of justice. Second, the authors discuss the implementation of strategies to articulate the public domain and propose intermediate, anchoring institutions at the meso-level by building ontologies, selecting technical functionalities and algorithms, and embedding protections of the rule of law into specific public health data ecosystems.

What the authors suggest in this paper is a new regulatory framework for the new data-driven technology with the potential to fully release its benefits for doctors, patients, hospitals, and the NHS at large (Lokshina & Lanting, 2019, 2023). A linked democracy perspective would focus, in this case, on emerging institutional-level concerns and pose questions such as: how can technology be designed? Can different stakeholders be involved in the design process and how? How can they distinguish and interact with both routinely inbound data and data that is newly produced? How new knowledge can be generated based on new data collected and information aggregated, circulated, and reused? What rules can emerge from this new public data ecosystem, and which meta-rules can frame it?

A linked democracy perspective assumes that deliberation, procedural rules, data, information, and knowledge cannot isolate from technology and its use and users; analyzing these particular interplays can shed further light on how broader democratic ecosystems must be developed. Therefore, the authors describe a broad conceptual landscape based on legal, political, ethical, and technical processes, which must be brought together to design a public space for linked data in a kind of distributed database system, called the web of data. Rather than analyzing concepts, or any in detail, they examine the interconnections between them with a focus on the conceptual interface. The authors outline frameworks for the theoretical building of the public space, and potentially, the notion presented by authors must lead to a better understanding of other related aspects, instead of a mere locking of concepts and developments in independent silos (Lokshina & Lanting, 2023).

The authors address certain issues involved in the construction of a public, open, and inclusive space, to discuss the legal and ethical implications of, among others, Big Data in public healthcare. The notion of public space should not be considered pertaining to the existing divide between public and private law as the authors refer here to the digital, social, and political space shared by citizens and involving state laws, technical standards, and government and corporate policies.

Over the past decade, deliberative and epistemic theories of democracy emphasized the importance of deliberation, procedural rules, information, and knowledge as essential components of the public domain. Democracy here is used in the sense of democratic governance involving all stakeholders. Building on these theoretical concepts, the authors suggest that the era of linked data also requires a new view of the democratic theory that focuses on a relationship between people, technology, and data (Casanovas et al., 2017; Lokshina & Lanting, 2023).

Linked data refers to a set of developments and standards for publishing data on the web. The term was proposed by Berners-Lee (2007) as a framework to connect data across websites and databases. The authors suggest the notion of linked democracy as a theoretical framework to map these connections and their emergent properties by looking at specific instances where these connections occur (Lokshina & Lanting, 2023).

As an example of issues to be addressed, consider the following event. Google's artificial intelligence unit called DeepMind began a business relationship in early 2016 with the Royal Free Hospital in the U.K., where part of their agreement involved creating an application that would help doctors to spot patients at risk of developing kidney disease. Google's DeepMind would in return have access to 1.6 million patient records from the U.K.'s NHS. The application concerned, first introduced at the Royal Free Hospital in 2017, raised almost immediate alarms from the Information Commissioner's Office (ICO), which investigated DeepMind's access to the mentioned medical data. To alleviate the issues, Google hosted a patient engagement forum "to work in closer partnership with the public" in late 2016 (Stevens, 2017).

Therefore, this paper is focused on the following research objectives. The authors evaluate if a linked democracy-based approach with safeguards implemented through meta-rule of law can enable better design of the regulatory models required to handle semantically driven data flows, including Big Data. Next, the authors investigate the connection with deliberative and epistemic democracy regulatory models focused on relationships between people, data, and institutions, where the meta-rule of law constitutes an analytical extension of the rule of law with the use of semantic languages. Lastly, the authors discuss the implementation of privacy, security, and data protection strategies in public health data ecosystems to shape the public domain with a new institutional framework covering ethical foundations for these strategies.

The emergent theoretical trend related to generating ecosystems within human-artificial environments is beyond the scope of this paper. However, the authors may be able to explore it soon because of a growing interest among researchers concerned about ethics, privacy, and data protection in computer science and artificial intelligence (Casanovas et al., 2021; Mendelson & Mendelson, 2017; Lokshina & Lanting, 2023).

Accordingly, the structure of the paper is as follows. Section 1 provides a literature review: it offers the background on data-intensive ecosystems and ethical frames for data and decisions; outlines the deliberative and epistemic democracy models and presents the linked democracy model as a potential regulatory instrument to frame properly the global public space. Section 2 explains how linked democracy and the meta-rule of law can provide the intermediate tools to integrate these models into specific data-intensive ecosystems at the meso-level by clarifying choices and decisions made in ontology-building for choosing the technical functionalities and algorithms; it also considers Electronic Health Record (EHR) systems as an appropriate example. Section 3 explains the implementation of regulatory models in public health data ecosystems: it associates the linked democracy regulatory model with specific data-intensive ecosystems such as eHealth; proposes the meta-rule of law as an effective regulatory framework to manage the semantic dimension of the web; and elaborates on embedding the protections of the rule of law into specific data-intensive ecosystems including direct, indirect, and tactic modeling of Privacy by Design (PbD); and outlines the ethical frames for public health data including complex equality, contextual integrity, ontology and informational ethics, and algorithmic governance. The final section provides concluding remarks about designing potentially improved regulatory frameworks to better represent and use public health data on the web of data in public health data ecosystems.

This paper is an extension of work presented at the Science Fiction Prototyping Conference (SCIFI-IT'2023), April 2–4, 2023, Ghent, Belgium, EUROSIS-ETI.

1. Related works

1.1. Data-intensive ecosystems and ethical frames for data and decisions

Consistent with complex system research (Badawi et al., 2014; Gutwirth & Leenes, 2016; Luo et al., 2016; Mathews, 2016; Pagallo et al., 2019; Casanovas et al., 2017, 2021; Lokshina & Lanting, 2019, 2021), it is concluded that entities cannot be sufficiently protected if the value of the entity needs to be protected or the consequences related to its loss are not well-understood. This is an important contextual direction and conclusion. Mathews (2016) indicated there can be many ways aimed at creating protection systems or applying protective regimes in line with developments depending on the various theoretical perspectives, ethical concerns, regulatory requirements, legal cultures, and commonalities and differences between national and international jurisdictions.

Despite an impressive body of investigations already performed, and increasing attention to these issues, there is no general agreement on what privacy factually means, and how safeguards should be implemented. There is no shared legal definition of Big Data either (Badawi et al., 2014; Lokshina & Lanting, 2018, 2023). Understanding the effects on people's lives and the associated regulatory impact on their social and legal status is an urgent task, recently addressed in many publications on health and data (Badawi et al., 2014; Luo et al., 2016; Lokshina & Lanting, 2019; Pagallo et al., 2019), data privacy (Casanovas et al., 2021; Lokshina & Lanting, 2021), data protection (Badawi et al., 2014; Gutwirth & Leenes, 2016; Pagallo et al., 2019; Casanovas et al., 2021; Lokshina & Lanting, 2021), applicable law (Hockings, 2016; Pagallo et al., 2019; Casanovas et al., 2021, 2023), and available computational ontologies (Casanovas & Poblet, 2021; Casanovas et al., 2021, 2023; Lokshina et al., 2018; Lokshina & Lanting, 2023).

While Big Data techniques and semantic analysis should not be confused as they entail different developments, it is linked data as the set of methods and standards for publishing data on the web, which is significant for both. As explained by Lokshina et al. (2018), Casanovas and Poblet (2021), semantic languages can not only connect documents or data fragments, for instance from APIs, but also things (i.e., objects). This linked world of things was the main notion behind the "single giant global graph", as one of the key visions of the web (Berners-Lee, 2007).

Benefits to biomedical informatics, biomedicine, and healthcare applications follow. The field of biomedical informatics is particularly active in this respect. For instance, Luo et al. (2016) stated that ProteomicsDB with a data volume of 5.17 TB includes 92% of the known human genes annotated in the SWISS-PROT protein sequence databank. The U.S. HITECH Act has nearly tripled the adoption rate of EHR in hospitals from 2009 to 2012 (Lokshina & Lanting, 2019). Data from millions of patients have already been digitally collected and stored (Lokshina & Lanting, 2019, 2023).

No doubt aggregated data can potentially improve healthcare services and increase research opportunities (Lupton, 2014; Lokshina & Lanting, 2021). However, the use and possible achievements of the web of data cannot be complete without warrants or other protections that should be established to guarantee the safety and security of individuals and organizations (Lupton, 2014; Hockings, 2016; Casanovas et al., 2021; Lokshina & Lanting, 2021). For instance, Lupton (2014) noted that information about patient experience generated new

avenues for commercial practices by enterprises that saw the opportunity to expropriate its value. In the new data economies of digital data generation and gathering, "the digital patient experience economy concentrates on the commercialization of written accounts or rankings by amateur people of their medical conditions, treatments, and interactions with healthcare providers". Casanovas et al. (2021) confirmed that inadequate people's "experiences and opinions as they are expressed in digital media forums, with all the suffering, hope, frustration, anger and joy that are often essential features of surviving medical conditions or handling medical procedures", have become commercial properties for commercial exploitation. Lokshina and Lanting (2021) explained that ordinary people are not offered financial compensation for providing their experiences; their contribution is non-commercial, while the value of the exchange of data they produce is accumulated by organizations that provide the platforms for patients to share their experiences or scan the web gathering data and presenting it in a form that is of value for commercial entities. Furthermore, Hockings (2016) informed that there is a regulatory shift in the governance of medical and biomedical data, "from a rights-based approach to the adjudication of competing claims, in which benefits of the economy are seen as goods to be balanced with data subject's right to privacy and confidentiality. These unprecedented levels of access by government and private sector actors give rise to new powers being used not in ways which reflect the interests of society as a whole, but rather in sectorial and government interests."

These are important issues. There is not always the need for data to be available immediately and to react quickly. The use of data in intensive care units is critical, while knowledge can increase with the secondary, less time-critical usage of clinical data (Badawi et al., 2014). Clinical support systems can benefit from the appropriate use of linked biomedical data. Translational tasks and actions make public health data more precise and efficient, including stored, transferred, and interoperable clinical data. Besides, preventing epidemics and infectious diseases becomes an urgent task in most regions of the world. For instance, based on the available online data, social media, and local news reports, an algorithm developed by Health Map indicated early signs of Ebola disease spread in West Africa nine days before they were clinically identified as "Ebola", even if the system used did not predict that the "mysterious disease" would spread (Lokshina & Lanting, 2021).

Therefore, the issues are not only in risks but also in encouraging business models that promote the use of data to change and meet requirements and challenges raised by Big Data. To be efficient, business models involving freemium, subscription, or commons developments cannot assume operating in unregulated open markets (Lokshina & Lanting, 2018, 2023). The authors believe that the objective of building sustainable ecosystems for the biomedical domain including public healthcare entails not only leveraging the use of data, but also the construction of its collective and public dimensions. This means rethinking such determinants as ethics, available democracy models, and the rule of law.

1.2. Deliberative, epistemic, and linked democracy regulatory models

In the 1990s, some political philosophers started putting public deliberation at the center of their democratic theories. The deliberative angle challenged the view of democratic practice

as a simple aggregation of voter preferences for representatives at elections. This new focus did not declare voting (i.e., the aggregation of preferences) as meaningless, but positioned it as a phase of deliberation in a democratic process (Bohman, 2009). As agreed by many researchers, deliberation is about "processes of judgment and preference formation and transformation within informed, respectful, and competent dialogue" with the essence of "inclusive, non-coercive and reciprocal discussion" on relevant issues that must "influence individual preferences and shape public policy" (Kuyper, 2015).

Based on these developments, some institutional innovations have been deployed at various levels of governance in democratic countries. These innovations, called "mini-publics", involve randomly selected microcosms of citizens that are convened to deliberate on public issues (Gronlund et al., 2014; Casanovas et al., 2017; Pagallo et al., 2019). Gronlund et al. (2014) provided cases of mini-publics including consensus conferences, planning cells, citizen juries, citizen assemblies, and deliberative polls.

Separate from these developments, another notion in the democratic theory emphasized the epistemic properties of democratic governance systems (Estlund, 2008; Landemore, 2013; Schwartzberg, 2015; Casanovas et al., 2017). For instance, Schwartzberg (2015) observed that epistemic democracy "defends the capacity of the many to make good decisions concerning an independent standard and seeks to justify democracy by reference to this ability". As the researcher explained, the epistemic model relies on the "four different historical and textual sources" such as Aristotle's "doctrine of the wisdom of the multitude"; Rousseau's link with Condorcet; Mill's utilitarian thought of the deliberative capacity of assemblies; and classical pragmatism (Schwartzberg, 2015).

Relevant supporters of the epistemic model are Estlund (2008) and Landemore (2013). As in the case of deliberative democrats, there was also diversity between epistemic democrats regarding what the standard of correctness in decision-making looks like. Estlund (2008) advised that "one version might say that there are right answers and also that democracy is the best way to get at them. Another version might say that there are right answers and there is value in trying collectively to get at them whether or not that is the most reliable way. Yet another version might say that there are no right answers independent of the political process, but it is best conceived as a collective way to know and institute what to do." Schwartzberg (2015) concluded that epistemic democracy "does not position itself as an alternative to deliberative democracy but instead generally repositions deliberation as being instrumental to meet the aim of careful decision-making."

Just as ad-hoc mini-publics were regarded as living labs to evaluate the theoretical principles of deliberative democracy, both epistemic democrats and their critics demanded more "empirical testing of the conditions under which groups of ordinary citizens are most likely to produce wise decisions" (Schwartzberg, 2015). Landemore (2013) informed that most evidence for the epistemic process has been provided through formal mechanisms like Condorcet's Jury Theorem (CJT) and its variants, or the Diversity Trumps Ability theorem (DTA).

However, neither deliberative mini-publics nor epistemic formal models include the contextual, intermediate level that shapes human decisions and ensures their implementation (i.e., the institutional layer of democratic systems). Human interactions within ad-hoc

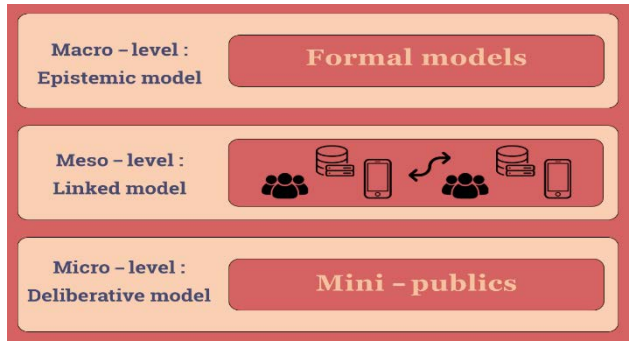

Figure 1. Deliberative, epistemic, and linked democracy regulatory framework with the linked model forming the meso-level (source: Lokshina & Lanting, 2023)

mini-publics do not occur in a vacuum and cannot disconnect from the organizations that create them, set their governing rules, and apply or ignore their carefully deliberated outcomes (Casanovas et al., 2017). Political agendas, policies, goals, expectations, and values are important parts of the picture. Similarly, epistemic formal models cannot fully grasp the emergent properties arising from the interaction between individuals and their contexts (Casanovas et al., 2017).

The democratic governance theory that dynamically links the distributed interactions between people, data, institutions, and both organizational and local contexts, provides a framework to analyze a missing intermediate level (Casanovas et al., 2017; Lokshina & Lanting, 2023). The authors relate this perspective, with its empirical load, to the linked democracy governance model that forms the contextual, intermediate level as shown in Figure 1 (Lokshina & Lanting, 2023).

2. Linked democracy and the meta-rule of law

2.1. Embedding safeguards into specific data-intensive ecosystems

The authors suggest that linked democracy and safeguards implemented through the meta-rule of law can provide the intermediate models to integrate the comprehensive models into specific platforms and applications, for instance, in use in the public healthcare domain. This intermediate modeling simplifies the choices and decisions made in building ontologies and selecting technical functionalities and algorithms. The authors refer to the institutional layer of democratic governance systems as they have already discussed (Lokshina & Lanting, 2023).

The meta-rule of law is a commonly used concept but may not be well-known under this name. It stands for a set of rules and agreements that provide a practical implementation of the law or laws it is associated with, providing guidance and avoiding many cases going to court; the latter is still an option for the parties involved. Rules applied by and agreements between insurance companies for insured cases of liability for damage are examples of a meta-rule of law application (Lokshina & Lanting, 2023).

Embedding specific protections into computer designs involves creating design tactics and including indirect strategies before modeling (Colesky et al., 2016; Casanovas et al., 2023; Lokshina & Lanting, 2023). A general rule is that regular audits of the system must be performed by an external supervisor and must be built within the ecosystem; this means to be designed, interpreted, supplied, and controlled by human agents possibly with the help of artificial agents. Colesky et al. (2016) defined the privacy design strategy as a distinct architectural goal in Privacy by Design (PbD) to attain a certain level of privacy protection. The researchers defined tactics as "an approach to PbD which contributes to the goal of an overarching privacy design strategy". As Colesky et al. (2016) explained, tactics represents an additional level of abstraction between strategies and privacy. Therefore, there is room for a wide range of computer modeling designs to "bridge the gap between data protection requirements set out in law and system development practice".

Koops and Leenes (2014) suggested, "privacy cannot be hardcoded." Lokshina and Lanting (2023) consider this to be a specific characteristic of all compliance with regulatory systems; however, law and ethics may not be suitable for hardcoding either. PbD is an important element in ensuring the protection of privacy, but it does not entail full protection. For instance, implementing the limited usage of personal information to reduce the impact of privacy violations, a principle introduced in the U.S. laws as well as in European General Data Protection Regulation (GDPR) and ISO 29100, requires something more than design strategies and tactics; it requires also to implement monitoring and external controls (Lokshina & Lanting, 2023).

Klitou (2012) noted that PbD is not a remedy as "laws or legal solutions do not perfectly regulate human behavior and neither do technologies or technical solutions." However, some challenges, limitations, and constraints of PbD can be addressed through the implementation of smart regulatory approaches and investment in necessary resources including training. The researcher acknowledged that serious threats and risks to privacy and liberty posed by the inertia of technological development are a vast dilemma for PbD or any legal or technical solution, "because no matter how privacy-invading technologies (PIT) are designed and developed, their widespread deployment and use are always a concern for the protection of privacy and liberty" (Klitou, 2012; Casanovas et al., 2017, 2021; Lokshina & Lanting, 2021, 2023).

The authors consider this issue from a legal perspective. The rule of law has two main dimensions to reduce these threats: enforcement of protections (specifically, binding rules) and social dialogue (particularly, citizen participation in creating norms, rules, and policies). Casanovas et al. (2017) identified and interpreted at least four growing regulation layers across both the dialogical (i.e., social) and binding (i.e., compulsory) axes of the rule of law including hard law (specifically, legislation and case law); multi-layered governance (predominantly, administrative and government policies); soft law (precisely, privacy impact charges, standards, and protocols); and ethics (particularly, ethical committees, fair information practices, and ethical theories). The researchers believe that to regulate data flows and bridge privacy and data protection, these regulation layers must be balanced and built into specific computer models and, also, included in existing institutional and legal designs (Casanovas et al., 2017, 2023; Lokshina & Lanting, 2023). The authors appropriately consider the use of Electronic Health Record (EHR) systems as an important example.

2.2. Electronic Health Record (EHR) systems

The EHR is an important aspect of digital healthcare, but at the same time represents a difficult combination of goals and requirements that must be met, from strict privacy and protection of sensitive data, medical history, and medication, to efficient access to close to real-time and complete information on the users current, or most recent, medical status. A new developing issue is that the content of an EHR could in some countries or regions lead to prosecution, e.g., in case of recorded drug use or abuse, even if in the past: this creates a dilemma for the completeness of the information in the EHR and thereby its value for the intended medical purpose.

In theory, national and regional EHR systems must involve all regulation layers. However, the promise that these systems, by providing instant, comprehensive, and accurate information about patients in clinical settings, must eliminate or minimize the risk of life-threatening medical errors, render unnecessary duplication of tests and procedures, and reduce consequent delays in treatment, has never fully emerged; furthermore, EHR interoperability is insufficient (Lokshina & Lanting, 2019, 2021, 2023; Mendelson, 2020). The information contained in each individual EHR may be incomplete, inaccurate, and counter-indicated for use in clinical settings. For instance, the Australian Digital Health Agency, the body responsible for the Australian national EHR system, called My Health Record, advised treating clinicians and healthcare providers "to assume that the information is not a complete record of a patient's clinical history" (Mendelson & Wolf, 2016; Casanovas et al., 2017; Lokshina & Lanting, 2019). As a result, only a very small number of general practitioners, and almost no medical specialists are known to use the system. However, the automated algorithm running the My Health Record scheme creates a new record every 38 seconds. These records include clinical summaries, specialist letters, referrals, prescriptions, and dispense records, automatically uploaded by General Practitioners (GPs). Pharmacies, public hospitals, other healthcare providers, and agencies are also users of the system. Although the My Health Record model is technically an "opt-in" scheme, very few patients are aware of the required consent to the virtually blanket uploading of their clinical records on the national system. Nor are the patients aware that among "participants" in the system allowed access and sharing of information contained in its records are the Veterans' Affairs Department, Defense Department, the Attorney-General's Department, and law enforcement entities (Mendelson & Wolf, 2016; Casanovas et al., 2017; Lokshina & Lanting, 2019).

In England, in 2013 the National Health Services (NHS) Trust created an EHR system called care.data, for social care information and highly sensitive medical records (Mendelson & Wolf, 2016; Casanovas et al., 2017; Lokshina & Lanting, 2019). Following serious privacy and security breaches caused its abandonment in 2016. Given the well-publicized scandals concerning breaches of security and privacy, many patients are less than enthusiastic about massive EHR schemes (Lokshina & Lanting, 2021).

At least concerning very large EHR systems, legal regulation alone is not sufficient to protect individual and collective rights, because, in the domain of personal health information, these systems create a massive power imbalance between patients and the state or system in favor of the latter. Can effective safeguards for medical data in electronic form ever be implemented?

At present, privacy, and specific legal requirements for privacy, are barely enforced. According to the survey on security and privacy literature (Mendelson & Wolf, 2016), only 8 percent of the reviewed articles referred to the training of health staff in security and privacy. The authors note the financial costs of data protection, as "it is clear from the findings that developing countries have currently proceeded with the adoption of EHR without any critical consideration for the security policy to protect EHRs." Social and political conditions also affect the implementation of technical requirements, and both concepts should not be mistaken (Mendelson & Wolf, 2016; Woods, 2016).

Systematic technical surveys of published research in EHR privacy and security show similar results: a lack of connection between the needs of stakeholders and technical solutions so that "barriers to the privacy and security protection of EHR systems persist" (Casanovas et al., 2017; Mendelson & Mendelson, 2017; Mendelson, 2020). Technical features have been identified in several ISOs and technical standards (e.g., ISO 29100 and ISO 27002). Among them are access control, compliance with security requirements, interoperability, integration and sharing, consent and choice mechanism, policies and regulation, applicability, and scalability, and cryptography techniques (Casanovas et al., 2017; Mendelson & Mendelson, 2017; Mendelson, 2020).

Many technical proposals focus on interoperability (Casanovas et al., 2017; Lokshina et al., 2019; Lokshina & Lanting, 2019, 2023; Mendelson, 2020). The authors distinguish systemic interoperability from semantic interoperability to meet computational sufficiency in Information Systems (IS) processing. Systemic interoperability means the ability of complex systems to interact, share, and exchange information. It concentrates on the coordination of practices including human behavior, organizational structures, tools, languages, and techniques (Lokshina et al., 2019; Lokshina & Lanting, 2019). Semantic interoperability means the ability to exchange and share information across computational systems (Lokshina & Lanting, 2023). This linguistic side should be integrated as a component of the social and organizational spaces to make interoperability more effective.

There is no doubt that EHRs will be widely adopted in the future. However, there are many issues to overcome. For instance, despite the increasing implementation of national and regional EHR systems, healthcare data has so far not been organized for intelligent data retrieval (Casanovas et al., 2021; Lokshina & Lanting, 2019, 2021; Mendelson, 2020). Mendelson and Mendelson (2017) made a distinction between three gradual stages for hospitals to show meaningful use: e-prescribing, patient Personal Health Records (PHRs) access, and access to comprehensive patient data. The researchers concluded that "the ground reality at this time is that the EHR interoperability is minimal".

Some recent reports linked interoperability with the openness of EHRs (Casanovas et al., 2017; Lokshina & Lanting, 2019, 2021, 2023). Openness means that "the data within an EHR should be available via programmatic interfaces for secondary use (e.g., data sharing between systems for research and population health)" which means that EHR developers must provide users with access to a copy of their current source code "to help mitigate healthcare business continuity problems if the developer goes out of business". For instance, a set of requirements EXTREME (EXtract, TRansmit, Exchange, Move, Embed) was defined for different use cases including clinicians, researchers, software administrators, and patients (Casanovas et al., 2017).

In 2010, Harvard Medical School and Boston Children's Hospital began an interoperability project to develop an innovative platform to enable medical applications across various health information systems. In 2013, they delivered the Substitutable Medical Applications and Reusable Technologies (SMART) platform that implemented clinical data models and an application-programming interface. SMART was described in the Fast Health Interoperability Resources (FHIR) standard. While SMART on the FHIR platform (by representing clinical data as resources and assuming that each resource is an expression of meaning stated in terms of fields and data types) appropriately addressed the requirements of end users and app developers, and provided open standards aligned with the requirements of clinical system vendors, it did not address legal and regulatory models to be included in interoperability testing (Casanovas et al., 2017; Lokshina & Lanting, 2023). Furthermore, the current state-of-the-art in EHR is merely giving access to static and semi-static information, while technology already allows access to "close-to-real-time" data, such as instantaneous blood pressure and SPO2 values, as is demonstrated by "smart watches".

2.3. Collective dimension of regulatory models in public health data ecosystems

While EHR technology intends to enable instant data-sharing among diverse parties in a secure manner, patients and doctors still will not trust these massive systems before they demonstrate adherence to the legal, ethical, and social values of the society they serve. These values can be debated and formed through citizen participation. One of the difficult problems that still need to be solved is how to combine citizens' knowledge and decisions with technical and expert knowledge. Another issue is how to share and discuss relevant political and ethical values (Lokshina & Lanting, 2021, 2023).

Constitutional provisions were used in the past to adequately include ethics and legal norms in the public healthcare domain (Casanovas et al., 2017). Referendums and polls are considered mechanisms of direct democracy; and when appropriately executed, they are also essential to deliberative democracy. They have a long provenance, particularly at the local government level. At the national level, depending on the constitutional structure of the country, there are three types of referendums: mandatory referendums on constitutional and non-constitutional matters launched by the Parliament (for instance, Switzerland); mandatory referendums on basic law (for instance, France, Ireland, Belgium, and Turkey) or constitutional amendments (for instance, Australia); and non-binding referendums (i.e., consultations).

Could a proposal for providing the constitutional guarantee of privacy and security concerning EHRs be the subject of a referendum? Theoretically, it could; however, it would depend on national legal systems. For instance, in Australia, mandatory referendums must be initiated by the Federal Parliament, i.e., by politicians. Given that the My Health Record Act 2012 allows the Australian government, without any substantial privacy and security protections, to constantly generate and aggregate data contained in shared EHRs, a referendum or a plebiscite on eHealth records is unlikely to be put to the vote (Mendelson & Wolf, 2016; Mendelson & Mendelson, 2017).

However, participation and people's comments and votes become not only technically feasible but increasingly relevant in health policy and business. The relationship between crowdsourcing and healthcare was known due to the open innovation platform InnoCentive since 2006; currently, more than 35 businesses and initiatives participated. Casanovas et al. (2017) found eight categories with solutions ranging from patient-caregiver connectivity and collaborative consumption related to economic models involving sharing goods or services by a group, to contagious disease surveillance. These categories include clinical innovation; virtual visits; caregiver connectedness; EHR and practice management; collaborative asset consumption; data visualization and sharing; collaborative learning, sharing, social benefit; and disease surveillance. The researchers advised it brings a cultural change. They noted that "qualitative changes in mindset may be a forerunner to institutional recasting as individuals increasingly take the responsibility to self-manage health in a more empowered proactive manner. The individual has become the central focal point in health, which is now seen as a systemic complexity of wellness and prevention, as opposed to an isolated condition or pathology. Not only is scientific advance critical, but also the philosophical and cultural context for moving away from the fix-it-with-a-pill mentality to the empowered role of the bio citizen in achieving the personalized preventive medicine of the future." The so-called "quantified self", citizen sensing, and the wide use of mobile applications cannot be ignored and are especially significant in non-Western cultures to foster social development and human welfare (Pagallo et al., 2019; Casanovas et al., 2021; Lokshina & Lanting, 2021).

The health crowdsourcing researchers advise that standardized guidelines are needed on crowdsourcing metrics that must be collected and reported to provide clarity and comparability in the procedural approaches (Pagallo et al., 2019; Casanovas et al., 2021; Casanovas & Poblet, 2021; Lokshina & Lanting, 2021). For instance, Casanovas and Poblet (2021) reached such a conclusion after reviewing various platforms for disaster management and Open-Source Intelligence (OSINT).

Lokshina and Lanting (2023) state that evidently the law cannot be ignored. Rights and open rights management are increasingly important to foster citizen participation and trust; however, implementing the rule of law on platforms and apps to regulate information flows requires another dimension to regulatory models which is different from standardization (Lokshina et al., 2018, 2020; Lokshina & Lanting, 2021, 2023).

For stakeholders to trust the EHR systems, the relevant institutions must be anchored within strong and transparent legal and ethical frameworks. The authors promote trust as a key element in the public healthcare domain concerning the relationship between the patients, doctors who upload confidential information on the EHR, and others who store, process, and distribute this data. An intermediate, "anchoring institution" means a set of legal rules, ethical values, and data protection principles included in the management of all platforms and applications through semantic languages, algorithms, and codes. Each crowdsourced platform for the EHR fosters establishing communities of end-users and stakeholders that require the enactment of a specific anchoring institution.

The communities are flexible, have distinctive features, and can create a conflict of interest to be solved not at the micro- or macro-level but at the meso-level where data flows operate instantiating linked data governance. Models of linked democracy must be implemented to

refine and put epistemic innovation and deliberative tools into practice. Therefore, the proposal extends beyond the notion of liberal democracy that depends only on voting and procedural strategies and connects the fundamental ethical models including complex equality, contextual integrity, ontology, informational ethics, and algorithmic governance.

2.4. Identity layer in public health data ecosystems

To enforce legal provisions and implement ethical principles identified by ethical trends and models, specific standards and protocols must align with them. This means that the notions defining what the individual is and what properties to use as an identity for the industry and governing agencies must change. What properties define the identity on the web? This issue is a complex and delicate one: should an identity on the web and health be combined, and what would be the relation to an identity associated with citizenship and nationality under national and international rules and laws, further complicated by multiple nationalities, migration, etc?

Lokshina and Lanting (2021) suggested that adapting legal protections to the notion of digital identity requires redefining the identity ecosystem layer. Digital identity, access management, and common vocabulary must be defined consistently. The authors noted that the National Institute for Standards and Technology (NIST) of the U.S. Department of Commerce has worked on standardizing vocabulary and taxonomy for digital identity, its attributes, and associated concepts. In line with the metadata models, the next step can be assigning values to attributes. Some of the problems concerning assigning values to attributes are discussed in recent publications (Casanovas et al., 2021; Casanovas & Poblet, 2021). For instance, Casanovas et al. (2021) identified issues as attribute currency and specifically how concepts such as decay rate, freshness, and date since the last verification could affect confidence scoring; complications around the term consent in "individual consented", and how privacy enhancing requirements could be better instantiated in the metadata elements; concerns about terminology, particularly for "provenance", and the types of values allowable under "verification".

There is also an issue concerning the criteria for assigning values to attribute metadata. For instance, Casanovas and Poblet (2021) quoted the National Institute for Standards and Technology (NIST) Internal Report 8112 which defined a schema for a range of metadata for a subject's attributes. The researchers explained a metadata schema for attributes that could be established about an individual during an online transaction, to enhance access control policies, along with other components including verification, consent, and compliance with privacy data protection policies (Casanovas & Poblet, 2021). The five schema's categories are provenance (predominantly, origin, provider, and degree of reliability); accuracy (specifically, verifier and verification method); currency (basically, the freshness of the metadata); privacy (particularly, consent, acceptable uses, cache time to live, and data deletion date); and security classification (specifically, security level). The researchers noted that "attribute metadata are important, but it is the granular attribute value metadata – for example, information about attribute values' reliability, the processes used to create or establish them, and the frequency with which they are refreshed – that is designed to enable greater trust across systems… Attribute metadata and attribute value metadata can be leveraged to enrich authorization decisions, facilitate cross-boundary interoperability and trust, and enable adoption of federated attributes" (Casanovas & Poblet, 2021).

In the quotation, the reference to interoperability assumes a semantic context only. However, it is a control system where access to benefits, records, and health services depends on the stored use of a pre-established but dynamic identity, which may depend on federated identity systems. Who can take control of such systems and what response and dispute resolution tools must be implemented to foster trust and monitor the performance of the individuals and groups?

The notion of linked democracy entails that the identity ecosystem layer can be given to citizens (bio citizens and digital citizens) under the protection of the meta-rule of law. Beyond security, reliability, and trust must also be the values obtained through cooperative means (Lokshina & Lanting, 2023). Recent publications suggest new initiatives reflecting constitutional crowdsourcing. For instance, the four dimensions of interacting legal modalities including laws, norms, market, and code can be developed using the identity wallet (Casanovas et al., 2017; Casanovas & Poblet, 2021; Lokshina & Lanting, 2021, 2023). The authors assume that the identity issue is a matter of political decisions rightly defending a person-centered perspective; however, it must be refined to stress the importance of ethics, privacy, and data protection for linked data. The challenge in coordinating the four dimensions of legal modalities is that a feasible system of rights also constitutes a set of issues to overcome. The boundaries of traditional tools built in the state respectively national sovereignty and customary international law must be balanced by the notion of global digital citizenship. However, currently, there is no consistent agreement on how to regulate the digital identity meta-system layer globally. Formerly, Tim Berners-Lee expressed similar concerns (Hardy, 2016; Casanovas et al., 2017).

3. Implementation of regulatory models in public health data ecosystems

3.1. Linked democracy regulatory model and public health data ecosystems

The linked democracy regulatory model is supported by linked data. It is a way to organize knowledge, institutions, and people to foster interoperability, remove silos, and create a protective framework for data sharing. It must operate by framing a relationship between the expert, collective, and personal knowledge in the biomedical domain including public healthcare (Lokshina et al., 2018, 2020; Lokshina & Lanting, 2023). The authors analyzed the case, considered in Chun and MacKellar (2012), of a typical user, Mary, who is researching clinical trials for her elderly father who is suffering from kidney cancer. Currently, the only way to get further information about a disease or treatment is that Mary would initiate a web search to find a definition or go through similar patients' experiences to get further information and decide. For instance, she would need to navigate over to PubMed and run searches to find relevant research papers. She could also go to a site like PatientsLikeMe and look for experiences and statistics on the drugs involved in the trial. Chun and MacKellar (2012) admitted that "a better solution is an integrated knowledgebase system that provides patients and caregivers with aggregated health information from various sources, so they can better understand diagnoses, alternative treatments, and side-effects of drugs. The large store of patient-generated content buried in medical social networking and blogging sites must be integrated into this knowledge base."

This is the simplest case assuming that Mary is provided with accurate and relevant information that helps her make health-related decisions. However, such an outcome cannot be realistically claimed or fulfilled in line with someone's expectations. It raises further professional and ethical concerns about the relationship between common and expert knowledge and about safety and medical decision-making.

How can knowledge be generated, stored, curated, managed, and transferred, including the deletion of medical information that is outdated, useless, or incorrect? Who is taking responsibility for the nature, volume, and quality of medical information which is available on the web? These questions raise non-trivial issues about liability, rights, and duties, beyond purely technical issues, and may even raise some confusion. The point is that linked data requires a democracy governance model able to handle information and knowledge (i.e., structured information) feasibly (Lokshina et al., 2018, 2020; Lokshina & Lanting, 2021, 2023). The authors noted that to implement a model, new regulatory tools are needed to anchor technical requirements and regulatory conditions into specific public data ecosystems (Lokshina & Lanting, 2021, 2023).

The integration of public and private resources is currently used to annotate, share, and reuse data with controlled vocabularies for multiple social, medical, and research purposes through computational ontologies. Staab and Studer (2003) defined ontology as a description of concepts and relationships (i.e., a formal program specification) available for an agent or a community of agents. Taxonomies are organized into graphs that let knowledge be structured, shared, and reused, with semantic languages like XML, RDF, or OWL, supporting the process.

Currently, the number and quality of biomedical ontologies have increased exponentially. Every aspect of the domain is covered: anatomy, cell types, phenotypes, chemical entities to annotate drugs and their biological activities, structures, and pharmaceutical applications for data interoperability, defined by Casanovas et al. (2017) as semantic interoperability that assumes generating a common sense or information exchange reference across computational systems. There are ontologies to facilitate capturing biomedical metadata that categorizes experiments by interpreting gene expression datasets and environmental conditions; classify human diseases by comparing data items and identifying meaningful biological relations between them; organize protein interactions to suggest candidate genes involved in diseases and repurpose drugs. Additionally, there are ontologies providing models for data interoperability from bench to bedside and for mobile applications (Casanovas, 2015; Casanovas et al., 2017; Casanovas & Poblet, 2021).

Many issues involving the security of databases, workflows, and the reuse of data by companies and governments have already been raised. Trust, safety, and security foster a person- or a patient-centered approach when the status of patients, experiences, expectations, and personal and environmental contexts define the provision of health services; "this way the patients turn from subjects of care to responsible managers of processes and conditions" (Casanovas et al., 2017; Casanovas & Poblet, 2021).

Patients and their families are citizens (bio citizens and digital citizens). Mary can be in touch with all sorts of patient associations, healthcare units, and health facilities. Meanwhile, Mary's search traces are picked up by automated data aggregators, on-sold, and can result in adverse consequences for Mary and her father in terms of health insurance, credit rating,

and employment (Lokshina & Lanting, 2023). Doctors, however, can profit from biobanks and medical-linked data (Casanovas et al., 2017; Lokshina & Lanting, 2023).

The authors believe that the rule of law is an invisible determinant of health. But the protections for the rule of law are filtered and interpreted through mediating algorithms together with annotation and ontology-building processes that frame the storage, management, interoperability, and reusability of data and metadata flows (Casanovas et al., 2017; Casanovas & Poblet, 2021; Lokshina & Lanting, 2023). Related public data ecosystems that have a global scope are regulated by an entangled and plural set of organizational protocols, standards, rules, and principles. Only a small set of them is specifically legal, about national or international bodies, and even these public data ecosystem rules require a more specific interpretation.

For instance, in international law, the Universal Declaration on Bioethics and Human Rights set the principles of informed consent; privacy and confidentiality; non-discrimination and non-stigmatization; respect for cultural diversity and pluralism; equality and justice; equity; solidarity and cooperation (UNESCO, 2005). The declaration states that "promotion of health and social development for their people is a central purpose of governments that all sectors of society share" and "the enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being without distinction of race, religion, political belief, economic or social condition." These principles are specifically significant for the U.S., but are of importance for all countries; however, there is no implementation agreement because state respectively national jurisdictions interpret the notion of social responsibility quite differently. Privacy is considered a fundamental right in Europe; in the U.S., under the Constitution, a right to privacy against governmental intrusion can be implied through the Bill of Rights (Casanovas et al., 2017; Lokshina & Lanting, 2023).

The authors noted that national sovereignty and state boundaries rank first. Customary international law is based on covenants, agreements, and pacts of a political nature between nation-states. The internet and the web of data emerged in a highly fragmented world where technology is qualified through the filtering of legal concepts shaped by different legal cultures and national jurisdictions (Casanovas et al., 2017; Casanovas & Poblet, 2021; Lokshina & Lanting, 2023). For instance, there is no common legal definition of metadata, which is sometimes referred to as secondary data (Casanovas & Poblet, 2021).

These are not fundamental problems, but the nature of law is quite diversified, context-related, and functionally dependent on power and types of governance. To manage it properly on the web, a meta-rule of law should be established to rebuild the public space and tailor specific privacy and data protection systems, where meta-rule of law refers to practices where rules and agreements based on the applicable laws are formulated and applied as tools to simplify and stimulate adherence to the underlying laws (Casanovas et al., 2017; Casanovas & Poblet, 2021; Lokshina & Lanting, 2023). This is not a question of discontent as safeguards are the same. The difference belongs to the instruments at hand. The use of computer ontologies and languages including digital rights management, rights expression languages, automated licenses, smart contracts, etc. have a regulatory effect that should be considered, acknowledged, and controlled at each step and level of implementation. Therefore, the meta-rule of law mirrors the original rule of law that requires controlling the implementation of algorithms

and uses of semantic languages from scratch (Aizenberg & van den Hoven, 2020; Casanovas et al., 2017; Casanovas & Poblet, 2021; Lokshina et al., 2019; Lokshina & Lanting, 2023).

Telemedicine, health surveillance, biobanks, epidemic controls, etc., all depend on data flows. How can be these flows regulated? For instance, the relationship between data flows and any singular person constitutes "a quantified self," where individuals deploy sensors and monitoring devices to monitor and try to improve their health (Barrett et al. 2013). The researchers proposed to expand and aggregate the concept to a population level, "leading to quantified communities that monitor the health and activities of their population, thereby improving collective health with a data-driven approach." Big Data can be used in both precision medicine (as prevention and treatment strategies that take individual variability into account, by linking EHR to molecular data) and disease prevention (through the integration of data about behavioral, social, and environmental risk factors as a technological underpinning of health-focused Big Data collected by sensors and smartphones to track aspects of health and health behaviors). Besides, legal controls must cover access, amount, quality, and degree of personal information involved in the generation, storage, management, and risk assessment not only at the content level but at the metadata level too (Aizenberg & van den Hoven, 2020; Barrett et al., 2013; Lokshina et al., 2018, 2020; Lokshina & Lanting, 2023).

Barrett et al. (2013) advised that "people tracking their weight, diet, or exercise routine and producing massive data should have the opportunity to monitor this data and make decisions." Lokshina and Lanting (2018, 2019) noted that converting unstructured data into its structured representation (i.e., information, knowledge) should occur transparently and responsibly. In making this happen, the citizens (bio citizens and digital citizens) will benefit from a more refined version of the rule of law that covers the tools and semantic languages to use to protect and manage citizens' rights on the web of data besides the principles and fundamental legal values.

3.2. Data protection and Privacy by Design (PbD)

Cavoukian and Chibba (2016) introduced seven principles of privacy, informing that privacy is: proactive; preventative; applied in the default setting; embedded into the design; providing full functionality; supporting end-to-end security; remaining visible and transparent; and user-centric, as well. The researchers distinguished between informational privacy and data protection. They considered that privacy is a much broader concept than data protection suggesting that "information privacy refers to the right or ability of individuals to exercise control over the collection, use and disclosure by others of their personal information, while data protection is generally established through a set of rules or legal frameworks that impose responsibilities on organizations that collect, use, and disclose personal information." Cavoukian and Chibba (2016) advised that data protection points to the collective dimension of the regulatory frameworks and refers to the rules governing both the monitoring and control of the implementation of the individual rights and responsibilities of public authorities. Meanwhile, information privacy as a broader concept, orthogonal to data protection, addresses security and self-management of personal information that can be transformed into Privacy by Design (PbD) when embedded into computational systems, for instance, full

attribution, data tethering, analytics on anonymized data, tamper-resistant audit logs, false negative favoring methods, self-correcting false positives, and information transfer accounting among others (Cavoukian & Chibba, 2016).

However, the relationship between the two dimensions is not evident as the link between them requires institutional and organizational mediation which is difficult to encompass and coordinate in advance. Besides, these dimensions are not fully bridged by applying automated methods either.

Despite existing regulations, pitfalls, privacy breaches, and all sorts of mistakes are quite common. For instance, in 2012, the supermarket chain Target's loyalty card of a teenage customer led the company's marketing analysts to predict and reveal that she was pregnant (Lokshina & Lanting, 2018). In 2016, the Australian Health Department published anonymous Medicare and pharmaceutical claims data that involved GPs and three million patients, or 10% of the whole Australian population (Middleton, 2016). The researcher indicated that deidentified records of claims under the Medicare benefits plan and pharmaceutical benefits scheme were made public under weak protection, presuming this would facilitate research. But it was easy to break the encryption algorithms using the same information, and this was what occurred. Besides, after reviewing Google Flu Trends (GFT), Casanovas et al. (2017) concluded that predictive analytics was prone to failure because large-scale applications based on logs about influenza were not accurate and reliable (Casanovas et al., 2017).

In mobile technology, Bruggemann et al. (2016) surveyed 476 mHealth (mobile eHealth) apps. The researchers reported that 105 apps requested personal information and used it to tailor the app experience in line with user preferences and needs; however, 21% of the apps collected personal information without any noticeable use for it, and 40% of the apps transferred personal information without encryption. Although the use of a secure, encrypted data link was not visible to users, a secure data link must permanently be used by mHealth/eHealth apps to guarantee the confidentiality and integrity of personal data.

Bruggemann et al. (2016) emphasized that informational privacy (in the context of accessibility and availability of information); personal privacy (in the context of personally identifiable information); territorial privacy (in the context of spatiality and temporality); and location privacy (in the context of geo-located information) must be supplemented by attributes relating to the ownership of hardware, explicit information, and metadata. Additional attributes like authorization, accountability, encryption, obfuscation, fragmentation, data-hiding, and social means, must be also included. Besides, there are issues raised by interdisciplinary research as privacy has many dimensions and distinctions associated with contexts, disciplines, methodologies, and tools (Lokshina & Lanting, 2021, 2023).

In the biomedical domain including public healthcare, genetic privacy, informed, dynamic, open consent, and constructing a consent matrix for Ethical, Legal, and Social Issues (ELSI) can play a significant role (Casanovas, 2015; Casanovas et al., 2017; Lokshina & Lanting, 2023). Woods (2016) suggested that these conceptual constructs constitute a rich and non-homogenous arena. Genetic privacy (i.e., the protection of genetic information from unauthorized disclosure) received "strong criticisms in favor of autonomy and research, with the principle of solidarity being balanced by the positive and negative effects of disclosure concerning the empowerment of patients and families." For instance, strategies for data sharing on rare diseases

are deemed to be "a necessity to ensure that patients can obtain a diagnosis and the potential for treatment" (Woods, 2016). The researcher specified that up to 80% of rare diseases are genetic diseases; therefore, strategies that seek to combine "omics" data with whole genome sequencing data, data from medical records, natural history data, and data on family members of the proband (i.e., affected individual) must be considered as critical research tools. Woods (2016) observed that a similar combination of data sources opens a potential for the exploitable repurposing of research data and presents the research participants with the challenge of consenting to a complex context of biomedical Big Data. However, this cannot occur unless appropriate measures to protect the patients and their families are used (Woods, 2016). All these trends, practices, and discussions are most relevant for constructing public spaces. In the web of data, such a space results from a complex relationship between agents, communities, and regulatory bodies, both public and private (Aizenberg & van den Hoven, 2020; Casanovas et al., 2017; Lokshina & Lanting, 2021, 2023). Lokshina and Lanting (2023) stated that the web of data is a knowledge-implemented space driven by computational techniques and practices.

Ontology Design Patterns (ODPs) are specifically developed to support reusability in engineering (Staab & Studer, 2003). Beyond domain and upper-top ontologies, ODPs are constructed to cluster relations between entities deriving from a stronger interaction between expert and computational design. Several ODPs are already built in biotechnology (Casanovas & Poblet, 2021). Gharib et al. (2016) informed about serious efforts to construct also high-level general ontologies for privacy and data protection with regulatory effects. It is only a matter of time before these efforts converge in public health data management and policy-driven strategies (Lokshina et al., 2019; Lokshina & Lanting, 2023).

Casanovas et al. (2017) described an ODP on license-linked data resources involving agents, rights, permissions, and prohibitions, ready to be reused for semantic web services.

The researchers stressed that "the specific features of semantic languages and algorithms not only expressed relations among entities but effectively built them up through hybrid machine/human/machine interactions" (Casanovas et al., 2017). Therefore, biomedical environments and scenarios including public healthcare ecosystems will depend on how well the conceptual modeling before computer design can be derived. For instance, the integration of non-ontological resources constitutes an issue for ontology-building reengineering (Casanovas et al., 2017). This cannot be achieved intuitively; this is therefore also a call for technically driven legal modeling with ethical and legal grounds.

3.3. Ethical frames for public health data ecosystems

From a regulatory point of view, data management like ontology building is not a neutral task. Values, principles, and moral beliefs are intertwined in technical decision-making and design modeling. Boddington (2016) stated that data is a moral vector; however, there is a risk in reducing the problem's complexity by "schematizing its conceptual dimensions into a passive and active agency according to a ruler/ruled attitude". Lokshina and Lanting (2023) developed a distinct perspective emphasizing four notions that conceptually frame the ethical field: complex equality, contextual integrity, ontology and informational ethics, and algorithmic governance. That way, the authors address the foundations for setting the relationship between linked democracy and the meta-rule of law; a descriptive stance follows.

3.4. Complex equality perspective

Walzer (1984) outlined the paradox of the liberal way of dividing society to foster individual liberties: "Liberalism is a world of walls, and each one creates a new liberty." As Walzer (1984) explained, "church, state, market, personal freedom, privacy, and family life were set apart during the past two centuries, and the current century inherited the walls." The issue was how to restore what was separated while acknowledging that in fact, people cannot jump easily over the walls. The researcher stated that "freedom is additive; it consists of rights within settings, and we must understand the settings, one by one if we are to guarantee the rights. Similarly, each freedom entails a specific form of equality or, better, the absence of a specific inequality of conquerors and subjects, believers and infidels, trustees and teachers, owners and worker, and the sum of the absences makes an egalitarian society" (Walzer, 1984).

Complex equality means that citizens must strike a balance for each of these separate realms; inequalities in the spheres of society should not interfere with each other. However, isolated settings do not exist. Instead, spheres of justice must be instated across distinct distributive spheres to respect the differences and harmonize social goods, wealth, political office, commodities, education, security, health, etc. Institutional integrity is at stake as a counterbalance to state power. Therefore, social goods must be distributed according to different standards and principles in different autonomous spheres (Walzer, 1984; Casanovas et al., 2017; Lokshina & Lanting, 2023).

3.5. Contextual integrity perspective

Walzer (1984) did not specifically focus attention on privacy and law but Nissenbaum (2010) did. Because of complex equality, the researcher suggested the concept of contextual integrity. Nissenbaum (2010) advised that the notion of contextual integrity "ties adequate protection for privacy to norms of specific contexts, demanding that information gathering and dissemination be appropriate to that context and obey the governing norms of distribution within", with three principles to apply such as protecting the privacy of individuals against intrusive government agents, restricting access to intimate, sensitive, or confidential information, and curtailing intrusions into spaces considered private or personal. The researcher explained that "a central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which anything goes, because things that we do, events that occur, transactions that take place happen in a context not only of place but of politics, convention, and cultural expectation" (Nissenbaum, 2010). Therefore, more specific contexts can be derived. The contexts are governed by norms that govern information suggesting two types of informational norms such as appropriateness and flow. Norms of appropriateness dictate what information about individuals is fit for disclosure in a particular context. Norms of flow regulate the information transfer from one party to another.

Nissenbaum's notion of contextual integrity relies on Walzer's pluralistic theory of justice, embracing that "contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated". Nissenbaum (2010) informs that with the internet and linked data, privacy threats have grown, and citizens must formulate operational norms to constrain what information websites can collect, with whom it can be shared, and under what conditions.

Both notions, complex equality, and contextual integrity, are highly influential among contemporary philosophers and computer scientists since contextual integrity can be formalized with linear-time temporal logic. Both perspectives can foster different trends of ethical guidelines for various domains, methodologies, and computer models because they contribute to blurring the stark dichotomy between public and private law (Casanovas et al., 2017). Specifically, these perspectives must be specified in technical requirements enriching various domains, especially in biomedical environments including public healthcare where these formulations cannot be ignored (Casanovas et al., 2017; Lokshina & Lanting, 2023).

However, the authors consider they are derived from a classical formulation of what is a subject, an individual or a group, for political and legal philosophy. Subject quality and identity must be treated separately; the issue is not with the contextual approach but with measures, strategies, and tactics implemented within digital environments.

3.6. Ontology and informational ethics perspective

Nissenbaum's contextual integrity is inflexible and regulatorily requirement. Mittelstadt and Floridi (2016) suggested a different ethical stance that is focused on ontology and information entities. The researchers introduced an ontological and epistemic turn in such a way that "agency becomes not human- but information-centered" (Mittelstadt & Floridi, 2016).

Mittelstadt and Floridi's notion reproduced four principles of informational ethics stating that entropy ought not to be caused in the infosphere; entropy ought to be prevented in the infosphere; entropy ought to be removed from the infosphere; then, the flourishing of the whole infosphere ought to be promoted by preserving, cultivating, and enriching their well-being (Mittelstadt & Floridi, 2016). After applying biomedical data, some guidelines intended for biobanks and translational medicine were suggested for the fourth principle, stating that "to make compatible the usage of biomedical data, privacy is not considered to hide the identities of human subjects but to foster something like the right boundaries for information turn" (Mittelstadt & Floridi, 2016). The researchers advised that monitoring the ecology of the infosphere means "balancing the decreasing of ontological friction and promoting the expansion and well-being of these entities" therein (Mittelstadt & Floridi, 2016).

Mittelstadt and Floridi (2016) informed that analysis of biomedical Big Data must differentiate the levels of abstraction to identify group harm, and ethical harm, and to assess the importance of epistemology in Big Data ethics. Therefore, translational medicine and the need to support the management of biobanks and informational, technical, and social flows are treated as different dimensions of the same ethical perspective (Mittelstadt & Floridi, 2016). The only issue is how the rights can be implemented and managed effectively through quantitative data (Aizenberg & van den Hoven, 2020; Lokshina & Lanting, 2023). What is the link between Big Data, algorithmic governance, and ethics?

3.7. Algorithmic governance perspective

Lokshina and Lanting (2021) defined that algorithms are used to monitor and control iterative cycles of information in database flows. Algorithmic governance means governance by algorithms beyond the existing governance of algorithms. This is a new concept and a new

research domain. In the past, encryption and differential privacy experts strived to minimize the risks of deidentification (Lokshina et al., 2019). For instance, Apple embedded local differential privacy into its mobile phones so that no consumer content could reach the company (Lokshina & Lanting, 2021).

Gillespie (2014) informed that public relevance algorithms are developed "to select what is the most relevant from a corpus of data composed of traces from our activities, preferences, and expressions" to perform six important dimensions, for instance, patterns of inclusion (defined as "the choices behind what makes it into an index in the first place, what is excluded, and how data is made algorithm ready"); cycles of anticipation (defined as "the implications of algorithm providers' attempts to thoroughly know and predict their users, and how the conclusions they draw can matter"); evaluation of the relevance (defined as "the criteria by which algorithms determine what is relevant, how those criteria are obscured from us, and how they enact political choices about appropriate and legitimate knowledge"); the ability of algorithmic objectivity (defined as "the way the technical character of the algorithm is positioned as an assurance of impartiality, and how that claim is maintained in the face of controversy"); entanglement with practice (describing "how users reshape their practices to suit the algorithms they depend on, and how they can turn algorithms into terrains for political contest, sometimes even to interrogate the politics of the algorithm itself"); and production of calculated publics (unfolding "how the algorithmic presentation of publics back to themselves shape a public's sense of itself, and who is best positioned to benefit from that knowledge").

Lokshina and Lanting (2023) found that algorithmic governance created many non-solved challenges. The authors advised that ethics and legal protections must be designed into the systems that collect real-time personal health data (Lokshina & Lanting, 2019, 2023). For instance, co-utility and self-enforcement protocols are proposed to facilitate the coordination and control between agents in decentralized systems encompassing fairness; however, these are not yet implemented (Gillespie, 2014; Casanovas et al., 2017, 2021, 2023; Lokshina & Lanting, 2021, 2023). Significant reconstruction at the institutional level is required to achieve it.

Conclusions

Our current reality is that both corporations and governments collect vast amounts of data about individuals and take advantage of this data with the stated objective to reduce costs and gain efficiency. However, at the same time, surveys and reports show an increasing lack of confidence in media, business leaders, elected officials, and possibly also in non-elected officials (Lokshina & Lanting, 2021). Such development significantly affects public healthcare, a data-intensive environment that manages ever-increasing volumes of biomedical data resulting from medical data-generating technologies and must handle the associated issues in an appropriate, balanced, and citizen-centered way.

In this paper, the authors discussed the construction of a global public space to regulate the collection, storage, access, and use of biomedical data and metadata, at different levels and scales, to build sustainable public health data ecosystems, and address associated issues. This global public space can assist citizens to get control of information flows by

defining identity in public health data ecosystems and shaping the capacity to use the web of data, a knowledge-implemented space driven by computational techniques and practices, to get access to healthcare services and receive benefits and appropriate care. For instance, EHR systems require creating trust among hospitals, doctors, and patients; but much more must be done to develop a consistent link between technical requirements, social conditions, and ethical values. Broadly speaking, semantics must be considered a fundamental component of systemic interoperability; however, only semantics is insufficient to build sustainable public health data ecosystems.

Concentrating primarily on the application to public health data of a regulatory framework considered suitable for ICT, the authors evaluated a linked democracy governance model with safeguards implemented through meta-rule of law to enable better design of regulatory models and tools required to handle semantically driven data flows, including Big Data. They also investigated the connection with the deliberative and epistemic democracy regulatory models focused on relationships between people, data, and institutions, where the meta-rule of law constitutes an analytical extension of the rule of law with the use of semantic languages; and showed that a strategy based on the linked democracy governance model and safeguards, implemented through the meta-rule of law, ties well in with the deliberative and epistemic democracy regulatory models. Additionally, the authors analyzed privacy, security, and data protection issues, applying existing ethical and legal frameworks for public health data and the theory of justice. They explained the implementation of strategies to articulate the public domain and proposed intermediate, anchoring institutions at the meso-level by building ontologies, selecting technical functionalities and algorithms, and embedding protections of the rule of law into specific public health data ecosystems.

The interface between human and artificial properties of communities deserves further attention and is earmarked for further study. The modeling of crowdsourced, collective intelligence is the focus of normative multi-agent system (norMAS) attempts to generate ecosystems within human-artificial environments. This theoretical trend is beyond the scope of this paper; however, the authors may be able to explore it soon because of a growing interest among researchers concerned about ethics, privacy, and data protection in computer science and artificial intelligence.

References

Aizenberg, E., & van den Hoven, J. (2020). Designing for human rights in AI. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720949566

Badawi, O., Brennan, T., Celi, L., Feng, M., Ghassemi, M., Ippolito, A., Johnson, A., Mark, R., Mayaud, L., Moody, G., Moses, C, Naumann, T., Nikore, V., Pimentel, M., Pollard, T., Santos, M., Stone, D., & Zimolzak, A. (2014, August). Making big data useful for health care: A summary of the inaugural MIT Critical Data Conference. *JMIR Medical Informatics*, *2*(2), Article e22. https://doi.org/10.2196/medinform.3447

Barrett, M., Humblet, O., Hiatt, R., & Adler, N. (2013). Big Data and disease prevention: from qualified self to quantified communities. *Big Data*, *1*(3), 168–175. https://doi.org/10.1089/big.2013.0027

Berners-Lee, T. (2007, November). *Giant global graph*. https://web.archive.org/web/20160713021037/http://dig.csail.mit.edu/breadcrumbs/node/215

Boddington, P. (2016). Big data, small talk: Lessons from the ethical practices of interpersonal communication for the management of biomedical Big Data. In B. Mittelstadt & L. Floridi (Eds.), *Law, governance*

and technology series: Vol. 29. The ethics of biomedical data. (pp. 277–305). Springer. https://doi.org/10.1007/978-3-319-33525-4_13

Bohman, J. (2009). Epistemic value and deliberative democracy. *The Good Society*, *18*(2), 28–34. https://doi.org/10.1353/gso.0.0079

Bruggemann, T., Hansen, J., Dehling, T., & Sunyaev, A. (2016, September). *An information privacy risk index for mHealth apps.* Proceedings Annual Privacy Forum 2016. SSRN. https://doi.org/10.1007/978-3-319-44760-5_12

Casanovas, P. (2015). Semantic web regulatory models: Why ethics matter. *Philosophy and Technology*, *28*(1), 33–55. https://doi.org/10.1007/s13347-014-0170-y

Casanovas, P., Mendelson, D., & Poblet, M. (2017). A linked democracy approach for regulating public health data. *Health Technology*, *7*, 519–537. https://doi.org/10.1007/s12553-017-0191-5

Casanovas, P., Hashmi, M., & de Koker, L. (2021). The rule of law and compliance: Legal quadrant and conceptual clustering. In V. Rodríguez-Doncel, M. Palmirani, M. Araszkiewicz, P. Casanovas, U. Pagallo, & G. Sartor (Eds.), *Lecture notes in computer science: Vol. 13048. AI approaches to the complexity of legal systems XI-XII. AICOL AICOL XAILA 2020 2018 2020* (pp. 215–229). Springer. https://doi.org/10.1007/978-3-030-89811-3_15

Casanovas, P., & Poblet, M. (2021). Adding semantics to the legal domain. *La Trobe*. https://doi.org/10.26181/61109185d2007

Casanovas, P., Gonzalez-Conejero, J., & de Koker, L. (2023). Legal compliance by design (LCbD) and through design (LCtD): Preliminary Survey. *La Trobe*. https://doi.org/10.26181/22910891.v1

Cavoukian, A., & Chibba, M. (2016). Cognitive cities, Big Data, and citizen participation: The essentials of privacy and security. In E. Portmann & M. Finger (Eds.), *Studies in systems, decision and control: Vol. 63. Towards cognitive cities* (pp. 61–82). Springer, Cham. https://doi.org/10.1007/978-3-319-33798-2_4

Chun, S., & MacKellar, B. (2012, March). Social health data integration using semantic web. In *SAC '12: Proceedings of the 27th annual ACM symposium on applied computing* (pp. 392–397). https://doi.org/10.1145/2245276.2245351

Colesky, M., Hoepman, J., & Hillan, C. (2016). Critical analysis of privacy design strategies. *2016 IEEE Security and Privacy Workshops (SPW)* (pp. 33–40). https://doi.org/10.1109/SPW.2016.23

Estlund, D. (2008). Epistemic approaches to democracy. *Episteme: A Journal of Social Epistemology*, *5*(1), 1–4. https://doi.org/10.3366/E1742360008000191

Gharib, M., Giorgini, P., & Mylopoulos, J. (2016). *Ontologies for privacy requirements engineering: A systematic literature review*. ArXiv. https://doi.org/10.48550/arXiv.1811.12621

Gillespie, T. (2014, October). The relevance of algorithms. in T. Gillespie, P. J. Boczkowski, & K. A. Foot (Eds.), *Media technologies: Essays on communication, materiality, and society.* MIT Press. https://doi.org/10.7551/mitpress/9780262525374.001.0001

Gronlund, K., Bachtiger, A., & Setalas, M. (2014). *Deliberative mini-publics: Involving citizens in the democratic process.* ECPR Press.

Gutwirth, R., & Leenes, P. (2016). *Data protection on the move. Current developments in ICT and privacy/data protection*. Springer. https://doi.org/10.1007/978-94-017-7376-8

Hardy, Q. (2016, June). The web's creator looks to reinvent it. *New York Times*. https://www.nytimes.com/2016/06/08/technology/the-webs-creator-looks-to-reinvent-it.html

Hockings, E. (2016). Critical examination of policy. Developments in information governance and biosciences. In B. Mittelstadt, & L. Floridi (Eds.), *Law, governance and technology series: Vol. 29. The ethics of biomedical Big Data* (pp. 95–115). Springer. https://doi.org/10.1007/978-3-319-33525-4_5

Klitou, D. (2012). A solution, but not a panacea for defending privacy: challenges, criticism, and limitations of privacy by design. In B. Preneel & D. Ikonomou (Eds.), *Lecture notes in computer science: Vol. 8319. Privacy technologies and policy. APF 2012* pp. 86–110). Springer. https://doi.org/10.1007/978-3-642-54069-1_6

Koops, B.-J., & Leenes, R. (2014). Privacy regulation cannot be hardcoded. A critical comment on the "privacy by design" provision in data-protection law. *International Review of Law, Computers, and Technology*, *28*(2), 159–171. https://doi.org/10.1080/13600869.2013.801589

Kuyper, J. (2015). Democratic deliberation in the modern world: The systemic turn. *Critical Review*, *27*(1), 49–63. https://doi.org/10.1080/08913811.2014.993891

Landemore, H. (2013). *Democratic reason: Politics, collective intelligence, and the rule of the many*. Princeton University Press. https://doi.org/10.23943/princeton/9780691155654.001.0001

Lokshina, I., & Lanting, C. (2018). Addressing ethical concerns of Big Data as a prerequisite for a sustainable Big Data industry. *International Journal of Interdisciplinary Telecommunications and Networking*, *10*(3), 33–54. https://doi.org/10.4018/IJITN.2018070104

Lokshina, I., Lanting, C., & Durkin, B. (2018). IoT- and Big Data-driven data analysis services for third parties, strategic implications, and business opportunities. *International Journal of Social Ecology and Sustainable Development*, *9*(3), 34–52. https://doi.org/10.4018/IJSESD.2018070103

Lokshina, I., Gregus, M., & Thomas, W. (2019). Application of integrated building information modeling, IoT and blockchain technologies in system design of a smart building. *Procedia Computer Science*, *160*, 497–502. https://doi.org/10.1016/j.procs.2019.11.058

Lokshina, I., & Lanting, C. (2019). A qualitative evaluation of IoT-driven eHealth: knowledge management, business models and opportunities, deployment, and evolution. In N. Kryvinska & M. Gregus (Eds.), *Lecture notes on data engineering and communications technologies: Vol. 20. Data-centric business and applications* (pp. 23–52). Springer. https://doi.org/10.1007/978-3-319-94117-2_2

Lokshina, I., Lanting, C., & Durkin, B. (2020). Evaluation of strategic opportunities and resulting business models for SMEs: Employing IoT in their data-driven ecosystems. In M. Jennex (Eds.), *Knowledge management, innovation, and entrepreneurship in a changing world* (pp. 148–186). IGI Global. https://doi.org/10.4018/978-1-7998-2355-1.ch007

Lokshina, I., & Lanting, C. (2021). A study on the wide-ranging ethical implications of Big Data technology in a digital society: How likely are data accidents during COVID-19? *Journal of Business Ecosystems*, *2*(1), 32–57. https://doi.org/10.4018/JBE.2021010103

Lokshina, I., & Lanting, C. (2023). Development of public health data regulatory models from a linked democracy perspective. In P. Geril & M. Polanska (Eds.), *Science fiction prototyping conference* (pp. 21–28). EUROSIS-ETI. Ghent, Belgium.

Luo, J., Wu, M., Gopukumar, D., & Zhao, Y. (2016). Big data application in biomedical research and healthcare: A literature review. *Biomedical Informatics Insights*, *8*, 1–10. https://doi.org/10.4137/BII.S31559

Lupton, D. (2014). The commodification of patient opinion: The digital patient experience economy in the age of Big Data. *Sociology of Health & Illness*, *36*(6), 856–869. https://doi.org/10.1111/1467-9566.12109

Mathews, R. (2016). On protecting and preserving personal privacy in interoperable global healthcare venues. *Health Technology*, *6*, 53–73. https://doi.org/10.1007/s12553-016-0126-6

Mendelson, D., & Wolf, G. (2016, December). "My electronic health record" – cui bono (for whose benefit)? *24 Journal of Law and Medicine*. SSRN. https://ssrn.com/abstract=2881787

Mendelson, D., & Mendelson, D. (2017). Legal protections for personal health information in the age of Big Data – a proposal for regulatory framework. *Ethics, Medicine and Public Health*, *3*(1), 37–55. https://doi.org/10.1016/j.jemep.2017.02.005

Mendelson, D. (2020). National electronic health record systems and consent to processing of health data in the European Union and Australia. In M. Corrales Compagnucci, N. Forgo, T. Kono, S. Teramoto, & E. Vermeulen (Eds.), *Legal tech and the new sharing economy. Perspectives in law, business and innovation* (pp. 115–131). Springer. https://doi.org/10.1007/978-981-15-1350-3_6

Middleton, K. (2016, October). Millions of Australians caught in health records breach. *The Saturday Paper*. https://www.thesaturdaypaper.com.au/news/politics/2016/10/08/millions-australians-caught-health-records-breach/14758452003833

Mittelstadt, B., & Floridi, L. (2016, April). The ethics of Big Data: Current and foreseeable issues in biomedical contexts. *Science and Engineering Ethics*, *22*(2), 303–341. https://doi.org/10.1007/s11948-015-9652-2

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Pagallo, U., Casanovas, P., & Madelin, R. (2019). The middle-out approach: Assessing models of legal governance in data protection, artificial intelligence, and the web of data. *The Theory and Practice of Legislation*, *7*(1), 1–25. https://doi.org/10.1080/20508840.2019.1664543

Schwartzberg, M. (2015). Epistemic democracy and its challenges. *Annual Review of Political Science*, *18*, 187–203. https://doi.org/10.1146/annurev-polisci-110113-121908

Staab, S., & Studer, R. (2003). *Handbook on ontologies*. Springer Science Business Media. https://doi.org/10.1007/978-3-540-24750-0

Stevens, L. (2017, March). Big read: What does Google DeepMind want with the NHS? *Digital Health*. https://www.digitalhealth.net/2017/03/deepmind-mustafa-suleyman-interview

UNESCO. (2005, October). *Universal declaration on bioethics and human rights*.

Walzer, M. (1984). Liberalism and the art of separation. *Political Theory*, *12*(3), 315–330. https://doi.org/10.1177/0090591784012003001

Woods, S. (2016). Big Data governance: solidarity and the patient voice. In B. Mittelstadt & L. Floridi (Eds.), *Law, governance and technology series: Vol. 29. The ethics of biomedical big data.* Springer. https://doi.org/10.1007/978-3-319-33525-4_10