Health Technol. (2017) 7:519–537
DOI 10.1007/s12553-017-0191-5

ORIGINAL PAPER

A Linked Democracy Approach for Regulating Public Health Data

Pompeu Casanovas[1,2] · Danuta Mendelson[3] · Marta Poblet[4]

Received: 17 October 2016 / Accepted: 6 April 2017 / Published online: 2 June 2017

Abstract This article addresses the problem of constructing *a public space* to build sustainable data ecosystems for the biomedical field. It outlines three models of democracy —*deliberative*, *epistemic*, and *linked*— where privacy and data protection can be explored in connection with the existing ethical frameworks for Public Health Data, and the Theory of Justice. For the construction of a sustainable public space, it suggests exploring the analytical dimension of *Linked Democracy*, and the need for building new tools to regulate 'Linked Open Data', based on rule of law and the analytical dimension of the meta-rule of law. The construction of 'intermediate' or 'anchoring' institutions would help in embedding the protections of the rule of law into specific ecosystems (including direct, indirect and tactic modelling of privacy by design).

Keywords Linked democracy · Privacy by design · Meta-rule of law · Web of data · Electronic health records · Identity

1 Introduction

Public Healthcare has traditionally been a data-intensive environment. Yet, the increased affinity toward big data, and its related analytics offer unprecedented opportunities for patients and many other stakeholders. The aforementioned opportunities include the discovery of trends in Public Health, diagnosis and treatment of diseases, patient care, public policy design, etc. At the same time, approaches and means of production, analysis, and combination of big datasets raise new challenges: How to build data ecosystems that effectively address the needs of the multiple stakeholders? Which tools, standards, and regulatory instruments will need to be developed, to make supportive ecosystems efficient, sustainable, and compliant with different legal and ethical frameworks?

This paper addresses some of the issues involved in the construction of a public, open, and inclusive space, to discuss the legal and ethical implications of Big Data in Public Healthcare.[1]

Deliberative and epistemic theories of democracy over the last three decades have stressed the importance of deliberation, procedural rules, and both information and knowledge as essential components of the public sphere. Drawing from

This article is part of the Topical collection on *Privacy and Security of Medical Information*

✉ Pompeu Casanovas
pompeu.casanovas@uab.cat; p.casanovasromeu@latrobe.edu.au

Danuta Mendelson
danutam@internode.on.net

Marta Poblet
martapobletbalcell@rmit.edu.au

[1] Institute of Law and Technology (IDT), Faculty of Law, Autonomous University of Barcelona, Cerdanyola del Vallès, 08193 Barcelona, Spain

[2] Law and Policy Program: Data to Decisions Cooperative Research Centre and La Trobe Law School, La Trobe University, Melbourne, VIC 3086, Australia

[3] Key Independent Researcher, formerly Chair in Law (Research), School of Law Deakin University, Melbourne, Australia, VIC, Australia

[4] Graduate School of Business and Law, Royal Melbourne Institute of Technology, Melbourne, VIC, Australia

[1] Our notion of public space should not be understood according to the strong divide between public and private law. We are referring here to the digital, social and political space shared by citizens and involving state laws, government and corporate policies, and technical standards.

these theoretical tenets, we suggest that the era of Linked Data[2] also calls for a new approach to democratic theory that pays attention to the interplay between people, technology, and data. We posit the notion of *"Linked Democracy""* as a theoretical framework to map those connections, and their emergent properties by looking at specific instances where these connections take place.

Consider the following scenario: In early 2016, Google's Artificial Intelligence unit DeepMind began a business relationship with the Royal Free Hospital in the UK, where part of their agreement involved the building of an application that would help doctors to spot patients, potentially at risk of developing kidney disease. As part of the business agreement, DeepMind would also be accessing 1.6 million patient records from UK's NHS. The Streams application, first introduced at the Royal Free in February 2017, raised almost immediate concerns from the Information Commissioner's Office (ICO) [1], who began an investigation into DeepMind's access to medical data. To address these issues, Google hosted in late 2016 a patient engagement forum 'to work in closer partnership with the public' [2].

That which we have here, is a new data-driven technology with potential benefits for doctors, patients, hospitals, and the NHS at large. A *Linked Democracy* approach would focus in this case, on emerging institutional level concerns, and would pose questions such as: How has the technology been designed? Have the different stakeholders been involved in that process and how? How will they be able to both – distinguish and interact with: routinely inbound data, and data that is newly produced? How will new knowledge will be collected, aggregated, circulated, and reused? What rules could emerge from this new ecosystem, and which meta-rules may adequately frame it?

A *Linked Democracy* examination here suggests that deliberation, procedural rules, data, information and knowledge cannot be isolated from technology and its users, and that analysing these particular interplays can also shed further light on how broader democratic ecosystems can be built.

The authors shall describe herein, a broad conceptual landscape drawing on legal, political, ethical and technical approaches, all of which will be brought together to design the public space for Linked Data in a distributed database system (the so-called 'Web of Data'). Rather than analysing each concept, or any in detail, we shall analyse the interconnections between them. Our focus is on the conceptual interface. We outline frameworks for the theoretical building of a public space*,* and conceivably, the approach presented by the authors might lead to a deeper understanding of other aspects than the mere locking of concepts and approaches in independent silos.

The present article is organised as follows. Section 2 briefly introduces the space of e-Health. Section 3 summarises the notions of *deliberative* and *epistemic* democracy, and introduces the concept of *linked* democracy, in order to frame properly, the notion of *'a global public space.'* Section 4 focuses on e-health, and introduces the notion of meta-rule of law to manage the semantic dimension of the web. Section 5 elaborates on Data Protection and Privacy-by-Design (PbD). Section 6 describes four main ethical frames for Public Health data, and defines the concepts of *complex equality*, *contextual integrity*, *ontology* (informational ethics), and *algorithmic governance*. Section 7 discusses the way of integrating these broad models into specific ecosystems through computational modelling, and introduces the notion of identity ecosystem layer. We will focus on the example of Electronic Health Records (EHR). Finally, Section 8 draws some conclusions toward designing better regulatory frameworks for the better representation and use of Public Health in the Web of Data.

2 Situating the e-Health space

As complex systems scholar Robert Mathews [3] recently argued, "no entity can be protected adequately if the value of that which is to be protected, and/or the consequences related to its loss are not well understood." This is an important contextual direction. However, there are many ways of understanding how to put into place protective regimes, according approaches depend to different theoretical perspectives, ethical concerns, regulatory systems, legal cultures, and national and international jurisdictions.

In spite of the impressive body of work already performed, and the increasing attention that these problems have attracted, there is no general agreement on what *Privacy* actually means, and how it should be implemented. There is no shared legal definition for *Big Data* either [4]. Yet, understanding the causal effects on people's lives and the associated regulatory effects on their social and legal status is an urgent task. It has been recently addressed in books and Conferences on Health and Data [5] [6] [7] [8] [9] [10], on Privacy and Data Protection [11] [12] [13] [14], and in many scientific articles relating to both fields, including two *Semantic Web Journal* Special Issues, on Health Care and Life Sciences [15], and on the Law [16]. Additionally, the *Journal of Biomedical Semantics* is regularly updating the information on available computational ontologies.

While Big Data and Semantic Analysis should not be confused, as they entail different methodologies; "Linked Data" is significant for both. As explained by Heath and Bizer [17] semantic languages (such as RDF) not only connect documents and/or data fragments (e.g. from APIs), but also *things*, i.e. entities described in each data fragment on the web. This

[2] Linked Data refers to a set of methods and standards for publishing data on the Web. The term was famously proposed by Tim Berners Lee in 2006 as a framework to connect data across websites and databases.

'linked world of things', was the main idea behind Tim Berners-Lee's dream of a single *Giant Global Graph* [18].

Benefits to bioinformatics, biomedicine, and Health Care applications follow. The field of biomedical informatics is one of the most active in such a respect. As Luo et al. [5] state in their 2016 state-of-the-art report, Proteomics DB (with a data volume of 5.17 TB) covers 92% (18,097 of 19,62) of known human genes that are annotated in the *Swiss-Prot* database. USA HITECH Act has nearly tripled the adoption rate of electronic health records (EHRs) in hospitals to 44% from 2009 to 2012 [5]. Data from millions of patients have already been digitally collected and stored.

It is certainly true that aggregated data can potentially enhance health-care services and increase research opportunities [5] [19]. Yet, in practice, the achievements of the Web of Data cannot be complete without warrants, and other forms of protections that should be put in place to guarantee the safety and security for all individuals and organisations. To put it bluntly [20]:

> […] patient experience prosumption has generated new avenues for commercial endeavours by enterprises that have seen the opportunity for expropriating its value. In the new data economies of digital data production and harvesting, the digital patient experience economy hinges on the commercialisation of written accounts or rankings by lay people of their medical conditions, their treatments and their interactions with healthcare providers. Lay people's experiences and opinions as they are expressed in digital media forums, with all the suffering, hope, despair, frustration, anger and joy that are often integral aspects of coping or living with a medical condition or surgical procedures, have become commercial properties for market exchange. They are not offered and nor do they receive financial compensation for providing their experiences. The value they derive is non-commercial, while the exchange value of the data they prosume is accumulated by the companies that provide the platforms for patients to share their experiences or trawl the web to harvest the data and render it into a form that is valuable for commercial entities.

Edward Hockings states that there is a regulatory shift [21]: "We are witnessing a 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, for example, are seen as goods to be balanced with a data subject's right to privacy and confidentiality. These unprecedented levels of access by Government and private sectors, give raise to new powers to be used in ways which reflect the interests of society as a whole, but rather, sectional interests and those of Government."

These are some of the problems. However, we should not react too rapidly, and throw the baby out with the bath water. The use of data in intensive care units may be *critical* [20]. Knowledge increases the secondary usage of clinical data [5]. Clinical support systems can benefit from the appropriate use of linked biomedical data. Translational tasks and actions may render Public Health data more precise and efficient, including stored, transferred, and interoperable clinical data. Preventing epidemics and infectious diseases is an urgent task in most regions of the planet.[3]

Then, perhaps, the problems are not to be found solely in the risks, but in encouraging business models that drive data use ought to change – in order to meet the needs and challenges raised by big data. To be efficient, business models based on *freemium*, subscription or commons approaches cannot assume that they operate in unregulated open markets [23]. It is our contention that the objective of building sustainable ecosystems for the biomedical field entails not only leveraging the use of data, but the construction of its *collective and public dimension*. This means rethinking such elements as ethics, available models of democracy, and the rule of law.

3 Deliberative, epistemic, and linked democracy

In the early 1990s, a number of political philosophers started to situate public deliberation at the centre of their democratic theories. The so-called "deliberative turn" challenged the view of democratic practice as the simple aggregation of voter preferences for representatives at elections. This new focus did not render voting (or the aggregation of preferences) as meaningless, but situated the same, as "a phase of deliberation' in a democratic process [24]. Deliberation, most authors would agree, is about "processes of judgment and preference formation and transformation within informed, respectful, and competent dialogue" [25]. The ideal is that "inclusive, non-coercive and reciprocal discussion" on relevant issues should influence "individual preferences and shape public policy" [26].

Drawing from these developments, a number of institutional innovations have been deployed at different levels of governance in many democratic countries. These innovations, usually referred to as 'mini-publics' [27], involve randomly-selected microcosms of citizens that are convened to deliberate on public issues. Examples of mini-publics are consensus conferences, planning cells, citizen juries, citizen assemblies, or the more recent deliberative polls [28].

[3] E.g. Based on the available online data, social media and local news reports, an algorithm developed by Health Map indicated early signs of the Ebola disease spread in West Africa nine days before they were identified as 'Ebola' [22]. The Healthmap did not predict that the "mysterious disease" would spread.

In parallel to these developments, another line of thought in democratic theory has stressed the "epistemic" properties of democratic systems. From this perspective, Schwartzberg observes, "epistemic democracy defends the capacity of the 'many' to make correct decisions [with respect to an independent standard] and seeks to justify democracy by reference to this ability" [29]. As she notes, the epistemic approach relies on four different historical and textual sources: "(a) ancient Athens and Aristotle's argument for the "doctrine of the wisdom of the multitude"; (b) Rousseau and his connection with Condorcet; (c) utilitarian thought, particularly Mill's defense of the deliberative capacity of assemblies; and (d) classical pragmatism" [29]. Relevant proponents of the epistemic approach are Waldron [30], Estlund [31], Landemore [32], and Ober [33]. As is the case with deliberative democrats, there is also diversity between epistemic democrats with regard to what the standard of correctness in decision-making looks like. Thus, Estlund [31] explains:

> […] one version might say that there are right answers and 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: there are no right answers independent of the political process, but overall it is best conceived as a collective way of coming to know (and institute) what to do. There are others.

Ultimately, Schwartzberg [29] contends that "epistemic democracy does not position itself as an alternative to deliberative democracy but instead generally resituates deliberation as being instrumental to meet the aim of good, or correct, decision making". Just as ad-hoc mini-publics are regarded as living laboratories to test the theoretical principles of deliberative democracy, both epistemic democrats and their critics demand more "empirical testing [of] the conditions under which groups of ordinary citizens are most likely to produce wise decisions" [29]. To date, most of the evidence for the epistemic approach has been provided through formal mechanisms such as the Condorcet Jury Theorem (CJT) and its different variants, or the Diversity Trumps Ability Theorem (DTA) by Hong and Page [32] [34].

Yet, neither deliberative mini-publics, nor epistemic formal models include the contextual, intermediate level that shapes human decisions and delimits their implementation, that is, *the institutional layer of democratic systems*. Human interactions within ad-hoc mini-publics do not happen in a vacuum and cannot be disconnected from the organisations that create them, set their governing rules, and apply (or ignore) their carefully deliberated outcomes. Political agendas, policies, goals, expectations, and values are part of the picture too. Likewise, epistemic formal models cannot fully grasp the emergent properties arising from the interaction between individuals and their contexts. A theory of democracy dynamically linking the distributed interactions between people, data, institutions, and both organizational and local contexts would provide a framework of analysis of this missing intermediate level. We suggest denominating this approach *"Linked Democracy"* (Fig. 1).

4 Linked Democracy and e-Health

Linked Democracy is supported by *Linked Data.* It is a way to organise knowledge, institutions, and people in order to foster interoperability, remove silos, and create a secure framework for data sharing. It might operate to frame the connection between expert, collective, and personal knowledge in the biomedical field. Let's borrow a practical example from Chun and MacKellar [35]:

"Consider 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 treatments is for people like Mary to initiate a web search to find a definition or go through similar patients' experiences to get further information and to make a decision. For instance, she would need to navigate over to PubMed and run searches there to find relevant research papers. She might also go to a site like PatientsLikeMe and search the site looking for experiences and statistics on the drugs involved in the trial. A better solution would be an integrated knowledge base system that provides patients and caregivers with aggregated health information from different sources, so they can better understand diagnoses, alternative treatments and side-effects of drugs. It is especially important that the large store of patient generated content buried in medical social networking and blogging sites be integrated into this knowledge base."

This is the simplest example. It is assumed that Mary will be provided with accurate and relevant information that will help her to make health related decisions. However, such an outcome can neither be realistically demanded, nor satisfied according to someone's expectations. It raises further professional and ethical questions about the relationship between common and expert knowledge, and about safety and medical decision-making.

How can knowledge be produced, stored, curated, managed, and conveyed in a reasonable way, including deletion of medical information that is outdated, superseded, found inefficacious, or amounting to quackery? Who is taking responsibility for the nature, volume and the quality of medical information which is available on the web?

These questions raise puzzling and non-trivial issues about liability, rights, and duties, beyond pure technical issues. The point is that Linked Data requires a model of democracy able

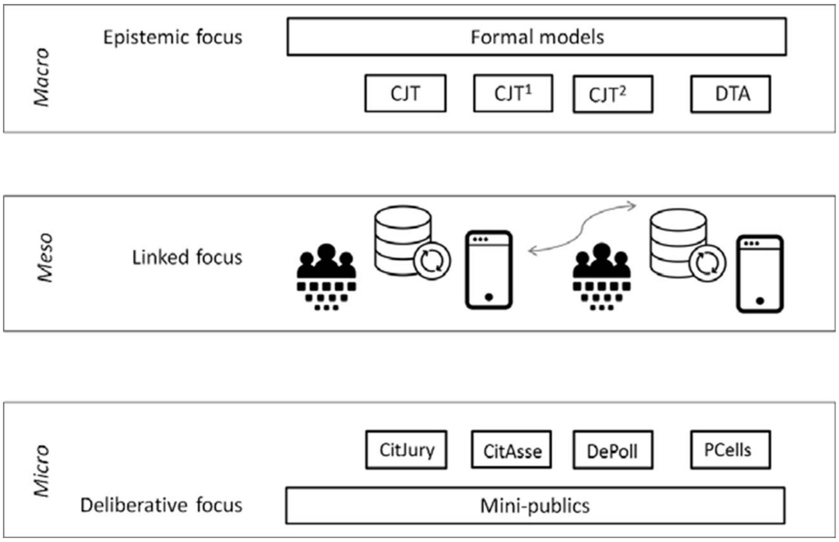

Fig. 1 Empirical focus of deliberative, epistemic, and linked democracy models

to handle information and knowledge (structured information) in a feasible way. But, to implement such a model we should take into account that new regulatory tools are also needed to anchor technical requirements and regulatory conditions into specific ecosystems.

The integration of public and private resources can be used at present to annotate, share and reuse data with controlled vocabularies for multiple social, medical, and research purposes. This is made possible by using *computational ontologies*. An ontology is a description (like a formal specification of a program) of concepts and relationships that can exist for an agent or a community of agents [36]. These questions raise puzzling and non-trivial issues about liability, rights, and duties, beyond pure technical issues. The point is that Linked Data requires a model of democracy able to handle information and knowledge —i.e. structured information— in a feasible way. But, to implement such a model we should take into account that new regulatory tools are also needed to anchor technical requirements and regulatory conditions into specific ecosystems. Taxonomies are organised into graphs that allow knowledge to be structured, shared, and reused. Semantic languages, such as XML, RDF and OWL, facilitate the process.

In the past few years, the number and quality of biomedical ontologies have increased exponentially. Almost every aspect of the field is being covered: anatomy, celltypes, and phenotypes; chemical entities to annotate drugs and their biological activities, structures, and pharmaceutical applications for data interoperability[4]; There are ontologies to capture bio-medical metadata to characterise experiments, for the interpretation of gene expression datasets, and for environmental conditions; ontologies to classify human diseases, to compare data items and identify meaningful biological relations between them; to identify protein interactions, to suggest candidate genes involved in diseases; to repurpose drugs [37]. There are several ontologies providing models that facilitate interoperability of data from bench to bedside [38] [39–41], and for mobile applications [42].

A number of issues about the security of databases, workflows, and the reuse of data by companies and governments have been raised already: What are the sign-on, access and authentication policies? Who handles testing, and how is it done? What encryption policies will protect data as it is transferred, or when it is being stored? Is there a single-tenant hosting option separated from that of other customers? Who manages the application on the back end, and what policies are in place to thwart insider breaches? What is the back-up and recovery plan? How well does the provider's security policy match companies? [43].

Trust, safety and security foster a person or *patient-centered* approach [44], in which, "the status of the patient, his/her experiences, expectations and wishes, but also his/her personal and environmental context define the provision of health services. By that way, the patient turns from subject of care to the responsible manager of processes and conditions. The new role of the patient must be accompanied by appropriate basic policies, frameworks and tools to enable the patient playing that role."

Patients and their families are citizens, and *digital* citizens. Mary may be in touch with all sorts of patient associations, health-care units, and health facilities. Obversely, Mary's search traces are picked up by automated data aggregators, on-sold and might result in adverse consequences for Mary and/or her father in terms of health insurance, credit rating or employment. Nevertheless, doctors can also benefit from biobanks and medical linked data.

[4] 'Interoperability' means 'semantic interoperability' here: the creation of a common meaning or information exchange 'reference,' across computational systems. We will be returning to this concept, later on (sections 7.1 and 7.3).

We agree with Richard Horton who, in 2016, has suggested in *The Lancet* [45] that the rule of law is an invisible determinant of health. But the protections of the rule of law are filtered and interpreted through the mediating algorithms and the annotation and ontology-building processes that frame the storage, management, interoperability, and reusability of data and metadata flows. The related ecosystems that have (or may have) a global scope, which are regulated by an entangled and plural set of organisational protocols, standards, rules and principles. Only a small set of them is specifically legal (pertaining to national or international bodies), and even these ecosystem rules require a more specific interpretation.

For example, in international law, the *Universal Declaration on Bioethics and Human Rights* (UNESCO, 2005) sets the principles of informed consent, privacy and confidentiality, non-discrimination and non-stigmatization, respect for cultural diversity and pluralism, equality, justice, equity, solidarity and cooperation. [46] Art. 14 states: "The promotion of health and social development for their people is a central purpose of governments that all sectors of governments that all sectors of society shares". Art. 14.1 recognises that "the enjoyment of the highest attainable standard of health is one of the fundamental rights of very human being without distinction of race, religion, political belief, economic or social condition".

The Declaration is specifically addressed to the States (art. 2). But there is no agreement about their implementation because national jurisdictions interpret the notion of social responsibility quite differently. Privacy is deemed to be a fundamental right in Europe; in the Supreme Court of the United States, Griswold v. Connecticut, 381 U.S. 479 (1965) determined that under the Constitution, a right to privacy against governmental intrusion can be implied through the Bill of Rights. Sovereignty and national boundaries ranks first. Customary international law is mainly based on covenants and pacts of a political nature between nation states—*pacta sunt servanda*. The Internet and the web of data emerged in a highly fragmented world in which technology is qualified through the filtering of legal concepts shaped from different legal cultures (e.g. common or civil law), and national jurisdictions. Yet, there is no common legal definition of 'metadata' (or 'secondary data' under UK legal terminology).

These are not obstacles, but the nature of law is quite diversified, context-related, and functionally dependant on power and types of governance. To handle it properly on the web, a *meta-rule of law* should be put in place to rebuild the public space and to tailor specific privacy and data protection systems [47]. This is not a question of discontent: protections are the same. The difference lies in the instruments at hand. The use of computer ontologies and languages —Digital Rights Management, Rights Expression Languages, automated licenses, smart contracts, etc.— have a regulatory effect that should be taken into account, acknowledged, and controlled at each step and level of implementation. Thus, the expression *meta-rule of law* mirrors the original rule of law, requiring the control of algorithm implementation and the use of semantic languages from the beginning.

Tele-medicine, health surveillance, bio-banks, epidemic controls etc., depend on data flows. How are these flows to be regulated? For instance, the relationship between them and any singular person constitute what has been referred to as a *quantified self*, where individuals deploy sensors and monitoring devices to measure and improve their own health. Barrett et al. [48] propose to expand and aggregate this concept to a population level, "leading to quantified communities that measure the health and activities of their population, thereby improving collective health with a data-driven approach". According to the authors, "big data" may be used both in precision medicine[5] (i.e. linking electronic health records to molecular data) and disease prevention (i.e. incorporating data about behavioural, social, and environmental risk factors): "the technological underpinning of health-focused big data is the use of sensors and smartphones to track various aspects of health and health behaviours" [48].

Barret et al. state that in addition, some legal controls should be put in place related to the access, amount, quality, and degree of personal information involved in the production, storage, management of, and access of their risk factors, not only at the content, but at the metadata level as well. People tracking their weight, diet, or exercise routine and producing passive massive data should have the opportunity to monitor this data, and to make decisions in relation to them. Converting unstructured data, into a structured representation of that data, should be done in a transparent and accountable fashion. But to make this happen, we could benefit from a more refined version of the rule of law, covering not only principles and fundamental legal values, but the tools and languages required to use, preserve, and manage citizens' rights on the Web of Data.

5 Privacy by design and Data Protection

Ann Cavoukian's seven principles of privacy are now well known.[6] She distinguishes between *informational privacy* and *data protection* [50]:

"Privacy is a much broader concept than data protection. 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. Data protection is generally established through a set of rules or legal frameworks that

[5] Precision medicine can be defined as the "prevention and treatment strategies that take individual variability into account" [49].

[6] A brief reminder: 1. Proactive not Reactive; Preventative not Remedial; 2. Privacy as the Default Setting; 3. Privacy Embedded into Design; 4. Full Functionality—Positive-Sum, not Zero-Sum; 5. End-to-End Security—Full Lifecycle Protection; 6. Visibility and Transparency—Keep it Open; 7. Respect for User Privacy—Keep it User-Centric.

impose responsibilities on organizations that collect, use, and disclose personal information".

According to her, 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 individual rights, and to the responsibility of public authorities. Privacy is a broader concept, orthogonal to data protection: it addresses the defence, and hetero- and self-management of personal information. It can be turned into Privacy by design when embedded into computational systems —i.e. Full Attribution, Data Tethering, Analytics on Anonymized Data, Tamper-Resistant Audit Logs, False Negative Favoring Methods, Self-correcting False Positives, Information Transfer Accounting [50] [51].

However, the connection between these two dimensions is not evident, as the link between them entails an institutional and organisational mediation that is difficult to encompass and coordinate in advance. Moreover these dimensions are not completely bridged using automated methods either.

In spite of existing regulations, pitfalls and privacy breaches are quite common, and it is easy to make all sorts of mistakes. In 2012, the supermarket chain Target 's loyalty card of a teenage customer led the company's marketing analysts to predict (and disclose) that she was pregnant [52] [53]. In 2016, the Australian Health Department published anonymous Medicare and pharmaceutical claims data involving GPs and three million of their patients (10% of Australian population). "De-identified" records of claims under the Medicare Benefits Schedule and Pharmaceutical Benefits Scheme were made public, assuming that this would facilitate research. But it was easy to break the encryption algorithms using the same available information, and this is what actually happened [54]. In addition, as Google Flu Trends (GFT) has shown, predictive analytics are prone to failure. Large scale applications based on logs relating to influenza are not completely accurate and reliable [55].

In mobile technology, the survey of 476 apps mobile health applications conducted by Brüggemann et al. [56] shows that 105 apps request personal information and use it to tailor the app experience according to users' preferences and needs:

> (….) 21% of the apps in our dataset collecting personal information collect it without any noticeable use for it. Privacy-attentive apps should only collect information actually used by the app to provide the app functionality or tailor the app to user preferences and needs. Otherwise, information collection appears fraudulent and leaves a negative overall impression of the app. 40% of the apps in our dataset transfer personal information without encryption. Even though use of a secure, encrypted data connection is not visible to users, a secure data connection should always be used by mHealth apps to guarantee confidentiality and integrity of personal data.

Information 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) should be complemented with properties regarding the ownership of hardware, explicit information, and metadata. Van de Ven and Dylla [57] identify some more properties: authorisation, accountability, encryption, obfuscation, fragmentation, data-hiding, and social means. Tsormpatzoudi et al. [58] stress the problems raised by interdisciplinary research: privacy has many dimensions and nuances according to contexts, disciplines, methodologies, and tools.

In the Public Health and bio-medical areas, genetic privacy [59], informed, dynamic, open consent, and the construction of a consent matrix for ethical, legal, and social issues (ELSI) may play a major role [60]. At present, these conceptual constructs constitute a rich and non-homogenous arena. Genetic privacy —the protection of genetic information from unauthorised disclosure— has received strong criticisms in favour of autonomy and research [61]. The principle of solidarity has been balanced with the positive and negative effects of disclosure regarding the empowerment of families and patients [62]. For instance, strategies for data sharing in rare diseases are deemed to be "a necessity to ensure that patients are able to obtain a diagnosis and the potential for treatment".[7] But this should not be done unless adequate procedures to protect patients and their families are in place. All these trends, experiences, and discussions are most relevant for the construction of a public space. In the Web of Data, such a space is the result of a complex interaction between agents, communities and regulatory bodies (either public or private). In other words, the Web of Data is a knowledge-implemented space, driven by computational techniques and practices.

Ontology Design Patterns [ODP] are specifically built to support reusability in engineering [63]. Beyond domain and upper-top ontologies, ODP are being constructed to cluster and better classify relations between entities, that stem from a closer cooperation between expert and computational design. Many of them have already been constructed in biotechnology [64] [65] [66]. There are serious attempts to build high general level ontologies for privacy and data protection with regulatory effects [67]. It is a matter of time before these common efforts converge in Public Health data management and policy-driven strategies.

[7] As stated by Woods [62]: "Up to 80% of rare diseases are genetic diseases and 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 (the affected individual) are now regarded as essential research tools. This combination of data sources opens a potential for the exploitable re-purposing of research data and presents the research participant with the challenge of consenting to a complex context of biomedical "Big Data".

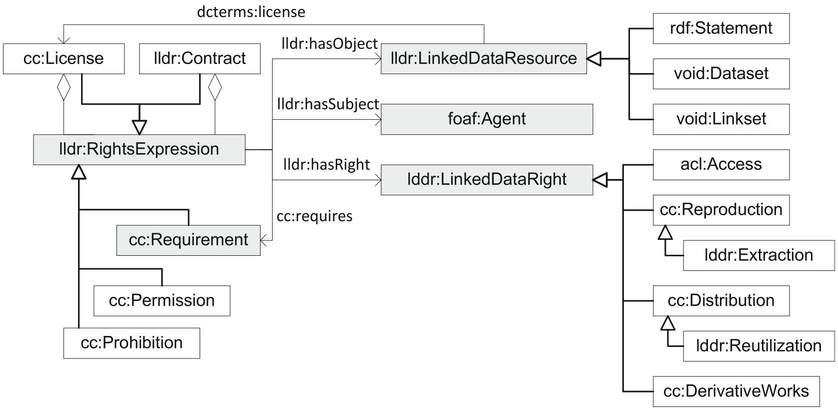

Fig. 2 Ontology Design Pattern for licensing [reproduced with permission]. Source: V. Rodríguez-Doncel, M.C. Suárez-Figueroa, M. Poveda, http://ontologydesignpatterns.org/wiki/Submissions:LicenseLinkedDataResources

We reproduce an ODP on license linked data resources comprising agents, rights, permissions, and prohibitions, ready to be reused for semantic web services (Fig. 2).

Our point is that the specific features of semantic languages and algorithms are not only expressing relations among entities, but actually *building* them up through *hybrid* machine/human/machine interactions. Thus, bio-medical ecosystems and scenarios will depend on how well the conceptual modelling previous to computer design can be drawn. For example, the integration of non-ontological resources constitutes a problem for ontology-building reengineering [68] [69] [70]. This cannot be done in an intuitive way: it is a call for technically-driven legal modelling with ethical and legal grounds[71][72].

6 Ethical frames for Public Health Data

From a regulatory point of view, data management, such as ontology building, is not a neutral task. Values, principles, and moral beliefs are intertwined in technical decision-making and design modelling. Perhaps this is what some researchers intend to mean when they state that *data is a moral vector* [73]. However, there is a risk in reducing the complexity of the problem by schematising its conceptual dimensions into a passive and active agency (i.e. a rulers/ruled approach). We are taking a different direction. We will highlight four notions to frame conceptually the ethical field: (i) *complex equality*, (ii) *contextual integrity*, (iii) *ontology* (not to be confused with computer *ontologies*), (iv) and *algorithmic governance*. Doing this, we intend to address the bases for setting the relationships between *Linked Democracy* and the *meta-rule of law*. In what follows, we will embrace a descriptive stance, followed by the discussion in the subsequent section (7).

6.1 Complex equality

"Liberalism is a world of walls, and each one creates a new liberty" [74]. The philosopher Michael Walzer points at the paradox of the liberal way of dividing society to foster individual liberties. According to him, church and the state, the market, familial freedom, privacy, and domesticity were set apart during the 18th and 19th centuries, and the 20th c. inherited the walls. His problem is how to reassemble what was separated, but acknowledging the fact that we cannot jump easily over the walls:

"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 workers—and the sum of the absences makes an egalitarian society."

Complex equality means that we need to strike a balance for each of these separate realms: inequalities in the several spheres of society should not interbreed, should not interfere with each other. However, isolated settings do not really exist. Instead, spheres of justice could be adjudicated across distinct distributive spheres, in order to respect the differences and harmonise social goods, wealth, political office, commodities, education, security, health, etc. Institutional integrity is at stake as a counter-balance to the state power. Therefore, according to Walzer, social goods may be distributed according to different standards and principles in different autonomous spheres [75].

6.2 Contextual integrity

Walzer did not specifically focus on privacy and law. Though, Hellen Nissenbaum does. Using *'complex equality'* as a starting point, she elucidates the notion of *contextual integrity.* According to Nissenbaum, 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" [76].

She introduces three principles to be applied: 1. Protecting privacy of individuals against intrusive government agents. 2. Restricting access to intimate, sensitive, or confidential information. 3. Curtailing intrusions into spaces deemed private or personal. However,

> "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." Almost everything —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."

Therefore, much more specific contexts can be drawn. She assumes that contexts are partially governed by norms that govern information, and she posits two types of informational norms: norms of appropriateness, and norms of flow or distribution. Norms of appropriateness dictate what information about persons is fit for disclosure in a particular context. Norms of distribution regulate the transfer of information from one party to another. This second notion leans on Walzer's pluralistic theory of justice. "contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated" [77].

With the Internet and linked data, threats to privacy have grown. Nissenbaum contends that we must formulate operational norms (a backdrop of context-specific substantive norms) that constrain what information websites can collect, with whom they can share it, and under what conditions [77] [78].

Walzer's and Nissenbaum's conceptualisations have proved to be highly influential — not only among contemporary philosophers, but in computer science too. Contextual integrity has been partially formalised using linear-time temporal logic [79].

Both approaches are powerful enough to foster different trends of ethical guidelines for many domains, methodologies and computer models, as they contribute to blur the stark dichotomy between public and private law. Notably, they can be specified in technical requirements cross-fertilising several domains (especially in bio-medical and Public Health environments). These formulations have not been ignored.

However, it can be shown that they stem from a classical formulation of what a subject (an individual or a group) is for political and legal philosophy. Subjectuality and identity should be treated separately. The problem does not lie in the contextual approach, but with the procedures, strategies and tactics to be put in place within digital environments. We will return to this later.

6.3 Ontology (informational ethics)

Contextual integration is prescriptive, regulatorily binding. Luciano Floridi takes a different ethical stance, focusing on *ontology* and information entities. There is an ontological and epistemic turn, then, one in which *agency* is not human, but information-centred [80].

Let's reproduce the four principles of Information Ethics: (i) entropy ought not to be caused in the *infosphere* (an environment that is populated by informational entities), (ii) entropy ought to be prevented in the infosphere, (iii) entropy ought to be removed from the infosphere, (iv) the flourishing of informational entities as well of the whole infosphere ought to be promoted by preserving, cultivating and enriching their well-being.

When applied to bio-medical data, with respect to the fourth principle, Floridi furnishes some guidelines for biobanks and translational medicine. To make compatible the usage of biomedical data, privacy is not deemed to hide, or to conceal identities of human subjects, but to foster something like the *right* boundaries for the information turn. Using Floridi's words, monitoring the ecology of the infosphere means "balancing the decreasing of ontological friction, and thus promoting the expansion and well-being of these entities in it" [81].

In their discussion of biomedical *Big Data*, Mittelstadt and Floridi differentiate the levels of abstraction that pertain to: (i) identifying group-harm ethical harms, (ii) assessing the importance of epistemology in *Big Data* Ethics. Thus, translational medicine, and the need for the taking *care* of both the management of biobanks and the informational technical and social flows, are treated as different dimensions of the same ethical perspective. The problem is: how, and in which way, rights can be implemented and managed effectively through quantitative data. What is the link between Big Data, algorithmic governance, and Ethics?

6.4 Algorithmic governance

Algorithms can be used to monitor, and to control iterative cycles of information within, and between, database flows. Algorithmic governance means governance *by* algorithms, in addition to already existing governance *of* algorithms. This is a new concept, and very likely, according to the New York University Conference held in May 16–17, 2013, a new field of research.[8]

In the last ten years, *encryption* and *differential privacy* experts have strived to minimize risks of de-identification [82]. Apple has just embedded "local" differential privacy into its mobile phones, so that no consumer content can reach the company [83].

Communication scholar Tarleton Gillespie [84] defines *public relevance algorithms* as "algorithms to select what is most relevant from a corpus of data composed of traces of our activities, preferences, and expressions". He identifies the following six dimensions:

[8] See http://governingalgorithms.org/

"(i) *Patterns of inclusion*: the choices behind what makes it into an index in the first place, what is excluded, and how data is made *algorithm ready; (ii) cycles of anticipation*: the implications of algorithm providers' attempts to thoroughly know and predict their users, and how the conclusions they draw can matter; (iii) *the evaluation of relevance*: 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; (iv) *the promise of algorithmic objectivity*: 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; (v) *entanglement with practice*: 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; (vi) *the production of calculated publics*: 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." [85].

Algorithmic governance is drawing a broad map of non-solved challenges. Ethics and legal protections can, and should be, designed into the systems that are collecting personal health data in real time. For instance, co-utility and self-enforcement protocols have also been proposed to facilitate the coordination and control between agents in de-centralised systems, encompassing fairness [85]. But this has not been implemented yet: to make it happen, significant rebuilding at the institutional level would be needed.

7 Discussion

It is our contention that *Linked Democracy*, and the protections of the meta-rule of law, can furnish the intermediate models to integrate these four broad models into specific platforms and applications. This intermediate modelling makes explicit the choices and decisions made in ontology-building, and in the selection of technical functionalities and algorithms. We are pointing at the *institutional layer of democratic systems* (see above, section 2).

Embedding specific protections into computer designs entails drawing design tactics [86] and the incorporation of indirect strategies before modelling [87]. Compliance with a general rule such as: "Regular audits of the system should be performed by an external supervisor" cannot be performed by the system itself, but has to be accommodated within the ecosystem that is being designed, interpreted, created, and handled by (human or artificial) agents. Colesky et al. [87] (i) define *privacy design strategy* as "a distinct architectural goal in privacy by design to achieve a certain level of privacy protection", (ii) and define *tactics* as "an approach to privacy by design which contributes to the goal of an overarching privacy design strategy". According to the authors, 'tactics' represents an additional level of abstraction between strategies and privacy. Thus, there is room for a wide range of computer modelling designs to "bridge the gap between data protection requirements set out in law, and system development practice".

Bert-Jaap Koops and Ronald Leenes have convincingly asserted that privacy cannot be hardcoded [89]. Actually, it is our contention that this is a specific characteristic of *all* regulatory systems: law and ethics cannot be hardcoded either [90]. Privacy by design (PbD) may be an important solution for ensuring the protection of privacy, but it does not entail full protection. For instance, to implement the limited usage of personal information to reduce the impact of privacy violations, a principle that is present in USA laws, European General Data Protection Regulation (GDPR) and ISO ISO 29100, requires something more than design strategies and tactics. Monitoring and external controls have to be put in place too. Thus, PbD is not a panacea [91]:

"Laws or legal solutions do not perfectly regulate human behavior and neither do technologies or technical solutions. Some of these challenges, limitations and constraints of PbD, however, can be potentially addressed through the application/implementation of 'smart regulatory approaches' and the investment in necessary resources and training. Nonetheless, the dire reality is that the serious threats/risks to privacy (and liberty) posed by the inertia of technological development is probably a dilemma simply too immense for PbD or any legal or technical solution alone. In the end, no matter how PITs are designed/developed, their widespread deployment and use will likely always be a serious cause for concern for the protection of privacy and liberty."

PITs stands for *Privacy-Invading Technologies*: "PITs mainly consist of technologies with (blatant or latent) surveillance capabilities or other technologies that disallow techniques/approaches for reducing privacy risks/threats" [91].

Let's consider this issue from a legal point of view. The rule of law has two main dimensions to reduce these threats: enforcement of protections (binding rules), and social dialogue (citizens' participation in the making of norms, rules, and policies). At least four escalating regulation layers can be identified and interpreted across both the dialogical (social) and binding (compulsory) axes of the rule of law: (i) Hard law (legislation and case law), (ii) Multi-layered governance (administrative and government policies), (iii) Soft law (Privacy Impact Assessments, standards, and protocols); (iv) Ethics (ethical committees, Fair Information Practices,[9] and ethical theories) [71]. To regulate data flows, and to bridge privacy and data protection, these layers should be not only balanced and incorporated into specific computer models, but

[9] See the Guidelines for the Protection of Privacy and Transborder Flows of Personal Data set by the Organisation for Economic Co-operation and Development (OECD), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

incorporated into existing institutional and legal designs too [72]. Let's put the example of Electronic Health Records (EHRs) (also referred to as Medical Health Records [MHR]) in Public Health.

7.1 Electronic Health Records

National and regional EHRs systems,[10] should, in theory, engage each of the above regulation layers. However, the promise that these systems, by providing instant, comprehensive and accurate information about patients in clinical settings would eliminate or minimise the risk of life-threatening medical errors; render unnecessary many tests and procedures, and consequent delays in treatment, did not materialise. The information contained in each individual EHR is incomplete, and thus inaccurate and counter-indicated for use in clinical settings. The Australian Digital Health Agency, for instance, the body responsible for the Australian national EHR system called My Health Record, advises treating clinicians and healthcare providers 'to assume [that] the information … is not a complete record of a patient's clinical history' [92]. As a result, only a very small number of general practitioners, and almost no medical specialists, have registered to use the system.

Yet the automated algorithm running the My Health Record scheme creates a new record every 38 s. These records include clinical summaries; specialist letters; referrals, prescription and dispense records automatically uploaded by General Practitioners. Pharmacies, public hospitals, other healthcare providers and agencies registered with the system.[11] Although the My Health Record model is nominally an "opt in" one,[12] very few patients are aware of let alone 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 to share information contained in its in its EMRs are the Veterans' Affairs Department and Defence Department, the Attorney-General's Department and law enforcement entities.[13]

In England, in 2013 the National Health Services Trust created an electronic EHRs for social care information and highly sensitive medical records (care.data): subsequent serious privacy and security breaches led to its abandonment in July 2016 [93]. Given the well-publicized scandals relating to breaches of security[14] and privacy, many patients are less than enthusiastic about massive EHRs schemes.

At least in relation to very large EHR systems, legal regulation alone is not sufficient to protect individual and collective rights. For in the domain of personal health information, these systems create a massive power imbalance between patients and the state in favour of the latter. Can effective protections for medical data in electronic form ever be set in place?

Privacy, and specifically legal requirements for privacy, are barely implemented. According to the survey carried out by Fernández-Alemán et al. on security and privacy literature [95], only 4 (8%) of the reviewed articles referred to training of health staff in security and privacy. Mahfuth et al. [96] interestingly note the financial costs of data protection, as "it is clear from the findings that developing countries have currently proceeded with the adoption of EMR without any serious consideration for the security policy to protect EMRs." Social and political *conditions* also affect the implementation of technical *requirements*, and both concepts should not be confused.

Systematic technical surveys on the literature on EMR privacy and security shed 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" [97]. Technical features have been identified in several ISOs and technical standards (e.g. ISO 29100 and ISO 27002). Among them: access control, compliance with security requirements, interoperability, integration and sharing, consent and choice mechanism, policies and regulation, applicability and scalability and cryptography techniques.

Many technical proposals focus on interoperability. We should distinguish systemic interoperability from semantic interoperability (to meet computational sufficiency in Information Systems processing). The former notion refers to the ability of complex systems to interact, share, and exchange information. It focuses onto the *coordination* of practices, including human behaviour, organizational structures, tools, languages, and techniques [98]. In the aforementioned context, semantic interoperability refers to the ability to exchange and share information across computational systems. This linguistic side should be integrated as a component into the social and organizational one to avoid reductionism and make interoperability effective.

There is no doubt that EHRs are, and will be in the future, widely adopted. Yet, there are many obstacles to overcome. For example, despite the increased implementation of EHRs, healthcare data has not been organized for intelligent data retrieval. Chalasani et al. [99] differentiate three gradual stages in which hospitals can demonstrate meaningful use: e-prescribing,

[10] For example national EHR systems have been set up in Australia, Denmark, Jordan, Saudi Arabia, Austria, and the Netherlands, while Canada Spain have adopted regional ("autonomic") models.

[11] See https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/Content/news-002 .

[12] The My Health Records Act 2012 (Cth) Sch 1 cl 2(1) provides for introduction of an opt-out option.

[13] *My Health Records Act 2012* (Cth) Sch 1 cl 8(1); *My Health Records Regulation 2012* (Cth) reg 4.1.2.

[14] See BBC News [94]: "Three US healthcare organisations are reportedly being held to ransom by a hacker who stole data on hundreds of thousands of patients. The hacker has also put the 650,000 records up for sale on dark web markets where stolen data is traded. Prices for the different databases range from $100,000 (£75,000) to $411,000".

patient Personal Health Records [PHR] access, and access to comprehensive patient data. In the end, they clearly state: "However, the ground reality at this time in the United States is that the EHR interoperability is minimal or non-existent".

A recent Report by Sittig and Wright [100] links interoperability with the openness of EHRs. 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)" and that "EHR developers should provide customers with access to an 'escrowed' copy of their current source code to help mitigate health care business continuity problems in the event the developer goes out of business". They define a set of requirements (EXTREME: EXtract, TRansmit, Exchange, Move, Embed) for different use cases —clinicians, researchers, software administrators, and patients.[15]

From 2010 on, Harvard Medical School and Boston Children's Hospital began an interoperability project with the goal of developing a platform to enable medical applications across different healthcare IT systems. Substitutable Medical Applications and Reusable Technologies (SMART) is "a technical and market experiment to test whether standards-based data models could gain sufficient EHR vendor interest to influence the trajectory of the industry" [101]. In 2013, they created a platform to implement clinical data models and the application-programming interface described in a new, openly licensed Health Level Seven draft standard called Fast Health Interoperability Resources (FHIR). They called it SMART on FIHR, representing clinical data as resources (each resource is an expression of meaning stated in terms of fields and data types). The platform addresses the needs of end users and app developers and provides open standards that aligns with the needs of clinical system vendors, but does not specifically address legal and regulatory models. We contend that this is an essential step that should be encompassed with interoperability testing [102].

7.2 The collective dimension: Direct democracy, legal instruments, crowdsourcing

Even if the EHR technology were capable of enabling instantaneous data sharing among diverse and multiple parties in a secure manner, these massive systems will not be trusted by patients and doctors unless and until they can demonstrate adherence to legal, ethical and social values of societies within which they operate. Such values could be debated and ascertained through citizen participation. One of the difficult problems that still needs to be solved is how to combine citizens' knowledge and decisions with technical and expert knowledge. Another one is how to share and discuss the relevant political and ethical values.

Constitutional provisions have been used in the past, and are still being used to adequately include ethics and legal norms in the Public Health domain. Referendums and plebiscites are considered mechanisms of direct democracy; and if appropriately executed, they can be vital to deliberative democracy as well. They have a long provenance, particularly at the local government level [103]. At the national level, depending on the constitutional structure of the country, there are essentially three types of referendums: (1) on constitutional and non-constitutional matters that are binding on the Parliament (for example, Switzerland); (2) binding referendums on basic law (for example, France, Ireland, Belgium, and Turkey); or constitutional amendments (for example, Australia); and (3) non-binding referendums (sometimes referred to as plebiscites) [104] [105].

Could a proposal for providing constitutional guarantee of privacy and security in relation to electronic health records be a subject of a referendum? Theoretically it could; but this depends on national legal systems. For example, in Australia, binding referendums have to be initiated by the Federal Parliament, that is, by politicians. Given that the My Health Record Act 2012 (Cth)[16] allows the Australian government, without any substantial privacy and security safeguards, to constantly augment and aggregate data contained in shared electronic health records, a referendum or a plebiscite on eHealth records is unlikely to be put to the vote [92] [106].

However, participation and people's comments and votes are becoming not only technically feasible, but increasingly relevant in health policy and business. The relationship between crowdsourcing and Healthcare goes back to 2006 and the open innovation platform *InnoCentive*; at present, more than 35 businesses and initiatives are on the way. C. Hoffmann [107] identifies eight categories with solutions that range from patient-caregiver connectivity and collaborative consumption (an economic model involving sharing goods or services by a group), to contagious disease surveillance: (i) clinical innovation, (ii) virtual visits, (iii) caregiver connectedness, (iv) EHR and practice management, (v) collaborative asset consumption, (vi) data visualisation and sharing, (vii)

[15] These are the capabilities that should be widely shared: (i) (EXtract): enabling any health care organization to create a new secondary-use database (e.g., for population health management or clinical research); (ii) (Transmit): enables a clinician to send a copy of a patient's record to another physician as part of a referral or to a patient's personal health record; (iii) (Exchange): enables a health care organization to participate in a community-wide health-information exchange; (iv) (Move) enables a health care organization to switch HER developers without incurring extraordinary data extraction and conversion costs; (v) (Embed) enables an organization to develop new EHR features or functionality and incorporate this new software into clinicians' workflow within their existing EHR.

[16] In November 2015, the Federal Parliament through *Health Legislation Amendment (eHealth) Act 2015* (Cth) substantially amended the *Personally Controlled Electronic Health Records Act 2012* (Cth) and renamed it *My Health Records Act 2012* (Cth).

collaborative learning, sharing, and social benefit; (viii) disease surveillance. This entails a cultural change [108]:

"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 biocitizen in achieving the personalized preventive medicine of the future."

The so-called 'quantified self' [108], 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 [109] [110] [111].

The health crowdsourcing literature reviewed by Boulos et al. concludes that "standardised guidelines are needed on crowdsourcing metrics that should be collected and reported to provide clarity and comparability in methods" [110]. A similar conclusion is reached by Poblet et al. [112] after the analysis of 27 platforms for disaster management and Open Source Intelligence (OSINT).

We strongly believe that law cannot be placed aside. Rights and open rights management will be increasingly important to foster citizens' participation and trust. But implementing the rule of law on platforms and apps to regulate information flows require another dimension to regulatory models that cannot be confused with standardisation, just as technical requirements cannot be confused with social conditions, or semantic interoperability with systemic interoperability. For stakeholders to trust EMR systems, the relevant institution must function (be anchored) within strong and transparent legal and ethical frameworks.

We use *trust* in the Health Care domain in the sense of relationship among patients, their doctors who upload confidential information on the EMR, and those who store, process and distribute this data. By *anchoring institutions* we understand the set of legal rules, ethical values, and data protection principles encompassed within the management of each platform and application through semantic languages (RDF, OWL, SPARQL…), algorithms, and codes. Each crowdsourced and OSINT platform —for disaster management, crisis mapping, citizens' political participation, or EMR— fosters the creation of specific communities of end-users and stakeholders that requires the enactment of a specific anchoring institution.

These communities are flexible, have different features, and can generate different conflicts of interests to be solved, not at the micro or macro-level, but at the *meso-level* in which dataflows operate. In other words, as stated in section 2: at the meso-level instantiated by linked data governance. Models of *Linked Democracy* can be implemented to refine and put epistemic innovation and deliberative tools into practice. This proposal (i) extends beyond the idea of liberal democracy relying only on voting and procedural approaches, (ii) links and bridges the main ethical models leaning on complex equality, contextual integrity, informational ethics, and algorithmic governance.

7.3 The Identity Ecosystem Layer

To apply legal provisions and implement the ethical principles set out by the ethical trends and models described above, specific standards and protocols should be aligned with them. This means that concepts defining what an individual is, and the properties to be used and computed (such as identity) for the industry, and governing agencies may need to change. What properties define what 'identity' is on the Web?

Adapting legal protections to the notion of digital identity requires redefining the *identity ecosystem layer.*[17] Digital identity and access management, and especially a common lexicon should be defined in a more consistent way. The National Institute for Standards and Technology (NIST) of US Department of Commerce is working on harmonizing and creating a more precise nomenclature and taxonomy for digital identity, its attributes, and associated concepts.

Assigning values to attributes, according to metadata models, constitute the next steps. The following are some of the problems that have been identified [114]:

"(i) Attribute currency and specifically how concepts such as decay rate, freshness, and date since last verification could affect confidence scoring; (ii) complications around the term consent in 'individual consented', and how privacy enhancing requirements could be better instantiated in the metadata elements; (iii) concerns about terminology, particularly with respect to 'provenance', and the types of values allowable under 'verification'".

The problem involves the criteria for assigning values to attribute metadata. *NIST Internal Report (NISTIR) 8112*: *Attribute Metadata,* defines a schema for a range of metadata for a subject's attributes [115]. It contains a metadata schema for attributes that may be asserted, about an individual during an online transaction, to enrich access control policies. Verification, consent, and compliance with privacy data protection policies are components of it. The five components (categories) of the schema are: (i) provenance (origin, provider, and pedigree-degree of authoritativeness), (ii) accuracy (verifier and verification method), (iii) currency (freshness of the metadata), (iv) privacy (consent, acceptable uses, cache time to live, and data deletion date), and (v) security classification (security classification level and releasability).

" (…) attribute metadata are important, but it is the *granular attribute value metadata* —for example, information about

[17] The idea of a meta-system identity layer for the Internet was first coined by Microsoft architect Kim Cameron ten years ago [113]. For the sake of simplicity, and thinking of implementation into specific domains in a public space, we use the expression "identity ecosystem layer".

attribute values' authoritativeness, 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." [115].

In the above quotation the reference to interoperability infers only a semantic context. In actuality this is a control system, in which access to benefits, records, and health services will depend on the stored use of a pre-established but dynamic identity, which may depend on *federated* identity systems. We may ask who is going to take control of such systems, and what response and dispute resolution tools will be put in place to foster trust and monitor their performance over individuals and groups. The notion of *Linked Democracy* entails that this *'identity ecosystem layer'* could, and should, be put into citizens' hands, and under the protection of the meta-rule of law. Beyond security, reliability and trust are the main values to be attained through cooperative means.

There are already many initiatives to reflect on *constitutional crowdsourcing*.[18] Lawrence Lessig addressed some of these problems and started a fruitful and most needed thread of legal thought already in 1999. The first version of his influential *Law and Other Laws of Cyberspace* (1999) did not take into account the different languages on which identity could be built. He addressed them in the (crowdsourced) second version of 2006. He stated that the four dimensions of interacting legal modalities —laws, norms, market, and physical architecture (code)— could be enriched with an identity "wallet" [116]. He acknowledged that this identity issue was a matter of political decisions, and he was right in emphasizing the importance of defending a person-centred perspective. However, this perspective should be refined to include the importance of ethics, privacy and data protection for Linked Data [117]. The complexity and difficulty in coordinating these four dimensions or legal modalities in an implementable system of rights constitute a set of obstacles to overcome. Perhaps the boundaries of traditional tools based in national sovereignty and customary international law could be balanced with a conception of global digital citizenship. Yet at this point in time, no consistent agreement has been reached about how to regulate globally the digital identity meta-system layer. Tim Berners-Lee and W3C representatives have recently expressed the same concerns [118].

8 Conclusions

Big Data is here to stay. We may use the Gartner definition of *Big Data:* "high-volume, high-velocity, and/or high-variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization". The volume of business data worldwide, across almost all companies, doubles every 1.2 years, and both companies and governments are collecting huge amounts of data about individuals to reduce costs and gain efficiency [119] [120]. Both take advantage of it, while existing surveys and reports in USA show an increasing lack of confidence in the media, business leaders and elected officials [121]. Virtually every type of cross-border transaction has a digital component. This means that *concepts* defining what an individual is, and the properties to be used and computed to define the *'identity ecosystem layer'* should be discussed and balanced.

In this article we have addressed the issue of creating a public space to regulate Public Health data and metadata at different scales and levels. I.e. helping individuals to get control over the information flow that will define the identity ecosystem and shape their capacity to operate on the web, to get access to health services, and to receive benefits and appropriate care.

(i). First, we have suggested that an approach based on the notion of *Linked Democracy* and protections implemented through *the meta-rule of law* can enable better understand and design the regulatory tools that are needed to handle semantically-driven big data flows.

(ii). We suggested that our approach correlates with the notions of deliberative and epistemic democracy, focusing on the relationships between people, data, and institutions. We state that the meta-rule of law constitutes an analytical extension of the rule of law, through semantic languages. Both aspects —political and legal— are complementary, and can contribute to the effective empowerment of citizens.

(iii). Third, we have discussed the implementation of privacy and data protection strategies to articulate the public domain. It is our contention that languages and tools of the web of data —vocabularies, ontologies, and Ontology Design Patterns, among others— have a strong regulatory effect on behaviour and might shape a new institutional framework

(iv). Fourth, we have provided the ethical foundations for such an approach. Complex equality, contextual integrity, informational ethics (ontology), and algorithmic governance, are at the grassroots of the *Linked Democracy* perspective. We have argued that *Linked Democracy* and the *meta-rule of law* can furnish the intermediate tools to integrate these models into specific ecosystems at the meso-level. This intermediate modelling makes explicit the choices and decisions made in ontology-building, and in the selection of technical functionalities and algorithms.

(v). Fifth, we have focused on the example of Electronic Health Records [EHRs]. To create *trust* among

[18] See e.g. http://constitutionlab.org/

hospitals, doctors and patients, further efforts should be devoted to make a consistent link between technical requirements and social conditions and ethical values. Semantics can be viewed as an essential component of systemic interoperability, but on its own, is not enough to build safe and reliable ecosystems.

The interface between human and artificial sides of communities deserves further attention. The modelling of crowdsourced, collective intelligence is at the grassroots of normative Multi-Agents Systems (norMAS) attempts to create ecosystems within human/artificial environments [122]. However, this theoretical trend is beyond the scope of the present article, though we may explore it in the near future. There is a growing research community developing Ethics, Privacy, and Data Protection in computer science and Artificial Intelligence.

Classical legal instruments such as voting, plebiscites, referendums, and constitutions still have the power of framing popular participation. Nevertheless, from a broader cultural perspective, it is arguable that the concepts of nation state and legality on which these instruments are grounded have proven to be too narrow to frame the regulatory trends emerging from the world Web of Data and the Internet of Things.

While we have not broached a more expansive vision of such liberal political notions coming from Enlightenment models such as 'individual', 'collectivity', 'subjectivity', etc., these could be redefined by the operational languages that constitute the identity ecosystem layer on the Internet.

Specifically in the Health Care domain, empowerment and the need of monitoring and controlling self-produced data have to find more personalised ways of handling and defining collective identities. The emerging public space cannot be conceived solely as an aggregation of individuals (or votes, roles, comments, and opinions). Rather, it must be based on the linking power of shared knowledge. Otherwise, "unregulated and rampant 'datafication' of identified or identifiable personal health information about individuals collected, managed, and disseminated without their knowledge and informed consent effectively treats data subjects – us – as mere means to an end." [123].

Acknowledgements Law and Policy Program of the Australian government funded Data to Decisions Cooperative Research Centre (http://www.d2dcrc.com.au/); Meta-Rule of Law DER2016-78108-P, Research of Excellence, Spain. In Figure 1, we used icons from the Noun Project: the group icon was created by Gregor Cresnar, the piled data icon by IcoDots, and the the mobile device icon by Vildana.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Funding Data to Decisions Cooperative Research Centre (D2D CRC Ltd., ABN 45168769677; Project DC160051-Integrated Policing: End User Evaluation. DER2016-78108-P. While the support of the Data to Decisions Cooperative Research Centre is acknowledged, the views expressed in this article do not necessarily reflect the views of the Centre.

Ethical approval This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent Informed consent was obtained from all individual participants included in the study (not applicable).

References

1. Stevens L. Big read: what does Google DeepMind want with the NHS? DigitalHealth 20 March 2017, available at: https://www.digitalhealth.net/2017/03/deepmind-mustafa-suleyman-interview/. Accessed 25 March 2017.
2. Wakefield J. Google Deepmind: should patients trust the company with their data? BBC news, 23 September 2016, available at: http://www.bbc.com/news/technology-37439221. Accessed 5 March 2017.
3. Mathews R. On protecting and preserving personal privacy in interoperable global healthcare venues. Heal Technol. 2016;6:53–73.
4. Casanovas P, de Koker L, Mendelson, D, Watts D. Regulation of Big Data: Perspectives on Strategy, Policy, Law and Privacy, Heath & Technology, Special Issue on Privacy, this volume.
5. Luo J, Wu M, Gopukumar D, Zhao Y. Big data application in biomedical research and Health Care: a literature review. Biomedical informatics insights. 2016;8:1–10. doi:10.4137/BIIII.S31559.
6. Bender E. Big Data in Biomedicine. Nature. 2015;527(7576):S1–1.
7. Raghupathi W. Data Mining in Healthcare. Healthcare informatics: improving efficiency through technology, analytics, and management. London: CRC Press; 2013.
8. Ye SQ, editor. Big Data analysis for bioinformatics and biomedical discoveries. Boca Ratón (USA): Chapman and Hall/CRC Press; 2016.
9. Goodman KW. Ethics, medicine, and information technology: Intelligent machines and the transformation of Health Care. Cambridge: Cambridge University Press; 2016.
10. Mittelstadt BD, Floridi L, editors. The Ethics of Biomedical data. Dordrecht: Springer; 2016.
11. Gutwirth S, Leenes R, de Hert P, editors. Reforming European Data Protection Law. Dordrecht: Springer; 2016.
12. Gutwirth R, Leenes PDH. Data Protection on the Move. Current Developments in ICT and Privacy/Data Protection. Dordrecht: Springer; 2016.
13. Gonzalez-Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Dordrecht: Springer; 2014.
14. Hijmans H. The European Union as Guardian of Internet Privacy. The story of art. 16 TFEU. Dordrecht: Springer; 2016.
15. Egaña-Aranguren M, Fernández-Breis JT, Dumontier M. Special issue on Linked Data for Health Care and the Life Sciences. Semantic Web Journal. 2014;5(2):99–100.
16. Casanovas P, Palmirani M, Peroni, S, Vitali F, van Engers, T. Guest Editors' Editorial: The Next Step. Special issue on the semantic web for the legal domain. Semantic Web Journal. 2016;7(3):213–27. doi:10.3233/SW-160224. Available at SSRN. https://ssrn.com/abstract=2765912. Accessed 25 March 2017

17. Heath T., Bizer C. Linked Data: Evolving the Web into a Global Data Space. Synthesis Lectures on the Semantic Web: Theory and Technology. Morgan & Claypool, 2011.
18. Berners-Lee T. Giant Global Graph. 2007-11-2. Available at: http://dig.csail.mit.edu/breadcrumbs/node/215. Accessed 12 October 2016.
19. Lupton D. The commodification of patient opinion: the digital patient experience economy in the age of Big Data. Sociology of Health & Illness. 2014;36(6):856–69.
20. Badawi, et al. Making Big Data Useful for Health Care: A Summary of the Inaugural MIT Critical Data Conference. MIR Med Inform. 2014 Jul-Dec. 2(2): e22. Published online 2014 Aug 22. doi: 10.2196/medinform.3447. Available at: http://medinform.jmir.org/2014/2/e22/?utm_source=TrendMD&utm_medium=cpc&utm_campaign=JMIR_TrendMD_0. Accessed 25 March 2017.
21. Hockings EA. Critical Examination of Policy-Developments in Information Governance. and the Biosciences. In B. D. Mittelstadt, L. Floridi, editors. The Ethics of Biomedical Data. Dordrecht: Springer, 2016, pp. 95–115
22. Asokan GV, Asokan V. Leveraging "Big Data" to enhance the effectiveness of "One health" in an era of Health Informatics. Journal of Epidemiology and Global Health. 2015;5(4):311–4. doi:10.1016/j.jegh.2015.02.001.
23. Bourne PE, Lorsch JR, Green ED. Perspective: Sustaining the Big-Data ecosystem. Nature. 2015;527(7576):S16–7.
24. Bohman J. Epistemic Value and Deliberative Democracy. The Good Society. 2009;18(2):s 28–34.
25. Dryzek JS., Niemeyer N. Deliberative Turns. In J. Dryzek, editor, Foundations and Frontiers of Deliberative Governance. Oxford Scholarship Online; 2009, pp. 3–17.
26. Kuyper J. Democratic deliberation in the modern world: The systemic turn. Critical Review. 2015;27(1):49–63.
27. Grönlund K, Bächtiger A, Setäläs M, editors. Deliberative minipublics: Involving citizens in the democratic process. Colchester: ECPR Press; 2014.
28. Fishkin JS. When the people speak: Deliberative democracy and public consultation. Oxford: Oxford University Press; 2009.
29. Schwartzberg M. Epistemic democracy and its challenges. Annual Review of Political Science. 2015;18:187–203.
30. Waldron J. The wisdom of the multitude: some reflections on book 3, chapter 11 of Aristotle's politics. Political Theory. 1995;23(4): 563–84.
31. Estlund D. Epistemic approaches to democracy. Episteme: A Journal of Social Epistemology. 2008;5(1):1–4.
32. Landemore H. Democratic reason: Politics, collective intelligence, and the rule of the many. New Jersey: Princeton University Press; 2013.
33. Ober J. Democracy and knowledge: Innovation and learning in classical Athens. Princeton University Press: Princeton; 2008.
34. Hong L, Page S. Groups of diverse problem solvers can outperform groups of high-ability problem solvers. Proc Natl Acad Sci. 2004;101(46):16385–9.
35. Chun SA, MacKellar B. Social Health Data Integration using Semantic Web, SAC'12, March 25-29, 2012, Riva del Garda, Italy, ACM, 2012, pp. 392–397.
36. Staab S, Studer R, editors. Handbook on Ontologies. Dordrecht: Springer Science Business Media; 2003.
37. Horridge M, Parsia B, Sattler U: The state of bio-medical ontologies. Bio-Ontologies SIG, 2011, http://bio-ontologies.knowledgeblog.org/135. Accessed 5 October 2016.
38. Hoehndorf R., Haendel M, Stevens R, Rebholz-Schuhmanns D. Thematic series on biomedical ontologies in JBMS: challenges and new directions. Journal of biomedical semantics. 2014; 5 (1): 1. doi: 10.1186/2041-1480-5-15, Available at: https://jbiomedsem.biomedcentral.com/articles/10.1186/2041-1480-5-15. Accessed 25 March 2017.
39. Luciano JS, Andersson B, Batchelor C, Bodenreider O, Clark T, Denney CK, Domarew C, Gambet T, Harland L, Jentzsch A, Kashyap V. The Translational Medicine ontology and Knowledge Base: Driving personalized medicine by bridging the gap between bench and bedside. Journal of Biomedical Semantics 2011 2(Suppl 2):S1. Available at: http://www.Jbiomedsem.Com/content/2/S2/S1. Accessed 5 October 2016.S
40. Machado CM, Rebholz-Schuhmann D, Freitas AT, Couto FM. The Semantic Web in Translational Medicine: Current applications and future directions. Brief Bioinform. 2015;16(1):89–103.
41. Sarkar I. N. Biomedical Informatics and Translational Medicine. Journal of Translational Medicine. 2010;8(1):1. doi: 10.1186/1479-5876-8-22
42. Olla P, Shimskey C. mHealth taxonomy: A literature survey of mobile health applications. Heal Technol. 2015;4(4):299–308.
43. Mohammed S, Fiaidhi J. Identifying the Emerging e-Health Technologies To Ubiquity 2.0 and Beyond. Ubiquitous Health and Medical Informatics. IGI Global, 2010.
44. Blobel B, Lopez DM, Gonzalez C. Patient privacy and security concerns on big data for personalized medicine Health and Technololy. 2016;6:75–81. doi:10.1007/s12553-016-0127-5.
45. UNESCO. Universal Declaration on Bioethics and Human Rights. 19 October 2005. 1260. doi:10.1016/S0140-6736(16)30061-7 Accessed 5 October 2016.
46. UNESCO. Universal Declaration on Bioethics and Human Rights. 19 October 20105. http://unesdoc.unesco.org/images/0014/001461/146180E.pdf. Accessed 5 October 2016.
47. Casanovas P. Conceptualisation of Rights and Meta-rule of Law for the Web of Data, Democracia Digital e Governo Eletrônico (Santa Caterina, Brazil). 2015;12:18–41; repr. Journal of Governance and Regulation. 2015;4(4):118–129.
48. Barrett MA, Humblet O, Hiatt RA, Adler NE. Big Data and disease prevention: from qualified self to quantified communities. Big Data. September 2013;1(3):168–75. doi:10.1089/big.2013.0027. http://online.liebertpub.com/doi/abs/10.1089/big.2013.0027. Accessed 5 October 2016
49. Collins FS, Varmus H. A new initiative on Precision Medicine. N Engl J Med. 2015;372(9):793–5.
50. Cavoukian A, Chibba M. Cognitive Cities, Big Data and Citizen Participation: The essentials of Privacy and Security. In: Portmann E, Finger M, editors. Towards cognitive cities. Switzerland: Springer International Publishing; 2016. p. 61–82.
51. Jonas J, Cavoukian A. Privacy by Design in the age of Big Data. Canada: Information and Privacy Commissioner, Toronto; 2012.
52. Duhigg C. How Companies Learn Your Secrets. The New York Times Magazine. 16 February 2012. Available at: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=0 Accessed 10 October 2016.
53. Vayena E., Gasser U. Strictly Biomedical? Sketching the Ethics of the Big Data Ecosystem in Biomedicine. In: B.D. Mittelstadt, l. Floridi, editors. The Ethics of Biomedical Big Data. Dordrecht: Springer; 2016, pp. 17–39.
54. Middleton K. Millions of Australians caught in Health records breach. The Saturday Paper. 8 October 2016. https://www.thesaturdaypaper.com.au/news/politics/2016/10/08/millions-australians-caught-health-records-breach/14758452003833. Accessed 8 October 2016.
55. Richterich A. Using Transactional Big Data for Epidemiological Surveillance: Google Flu Trends and Ethical Implications of 'Infodemiology'. In: B.D. Mittelstadt, l. Floridi, editors. The Ethics of Biomedical Big Data. Dordrecht: Springer; 2016, pp. 41–72.
56. Brüggemann T., Hansen J., Dehling T., Sunyaev A. An Information Privacy Risk Index for mHealth Apps. In: S.

Schiffner et al, editors. Annual Privacy Forum, APF 2016, Privacy technologies and policy, Frankfurt/main, Germany, September 7, LNAI 9857, Dordrecht, Heidelberg: Springer;2016, pp. 190–201.

57. van de Ven J., Dylla F. Qualitative Privacy Description Language. An Information Privacy Risk Index for mHealth Apps. In: S. Schiffner et al, editors. Annual Privacy Forum, APF 2016, Privacy technologies and policy, Frankfurt/main, Germany, September 7, LNAI 9857, Dordrecht, Heidelberg: Springer; 2016, pp. 171–189.

58. Tsormpatzoudi P., Berendt B., & Coudert F. Privacy by Design: From Research and Policy to Practice–the Challenge of Multi-disciplinarity. In: Annual Privacy Forum. Springer International Publishing. B. Berendt et al., editors, Third Annual Privacy Forum, APF-2015, Luxembourg, Luxembourg, October 7–8, 2015, Privacy technologies and policy, revised selected papers, LNAI 9484, Dordrecht, Heidelberg: Springer; 2015, pp. 199–212.

59. Hallinan D, De Hert P. Many Have It. Wrong–samples Do Contain Personal Data: the Data Protection Regulation as a Superior Framework to Protect Donor Interests in Biobanking and Genomic Research. In: The Ethics of Biomedical Big Data. Dordrecht: Springer; 2016. p. 119–37.

60. Woolley JP. How Data Are Transforming the Landscape of Biomedical Ethics: The Need for ELSI Metadata on Consent. In: Mittelstadt BD, Floridi L, editors, The Ethics of Biomedical Big Data. Dordrecht: Springer; 2016, pp. 171–197.

61. Goodman B. What's Wrong with the Right to Genetic Privacy: Beyond Exceptionalism, Parochialism and Adventitious Ethics. In: Mittelstadt BD, Floridi L, editors.The Ethics of Biomedical Big Data. Dordrecht: Springer; 2016, pp. 139–167.

62. Woods S. Big Data governance: solidarity and the patient voice. In: The ethics of biomedical big data. Dordrecht: Springer; 2016. p. 221–38.

63. Gangemi A., Presutti V. Ontology design patterns. In: Staab S, Studer R, editors. Handbook on ontologies. Berlin, Heidelberg: Springer; 2009, pp. 221–243.

64. Hoehndorf R., Ngonga Ngomo A-C., Pyysalo S., Ohta T., Oellrich A., Rebholz-Schuhmann D. Ontology design patterns to disambiguate relations between genes and gene products in GENIA. Journal of Biomedical Semantics 2011; 2 (5): S1. Available at: https://jbiomedsem.biomedcentral.com/articles/10.1186/2041-1480-2-S5-S1. Accessed 25 March 2017.

65. Egaña-Aranguren M, Antezana E, Kuiper M., Stevens R. Ontology design patterns for bio-ontologies: a case study on the cell cycle ontology. BMC bioinformatics 2008; 9 (5): S1. Available at: https://bmcbioinformatics.biomedcentral.com/articles/10.1186/1471-2105-9-S5-S1. Accessed 25 March 2017.

66. Seddig-Raufie D, Jansen L, Schober D, Boeker M, Grewe , Schulz S. Proposed actions are no actions: re-modeling an ontology design pattern with a realist top-level ontology. Journal of biomedical semantics 2012; 3 (2): S2.. Available at: https://jbiomedsem.biomedcentral.com/articles/10.1186/2041-1480-3-S2-S2. Accessed 25 March 2017.

67. Gharib M, Giorgini P, Mylopoulos J. Ontologies for privacy requirements engineering: a systematic literature review. The Computer Research Repository, CORR, November 2016. Available at: https://arxiv.org/abs/1611.10097. Accessed 17 February 2017.

68. Suárez-Figueroa MC, Gómez-Pérez A, Motta E, Gangemi A, editors. Ontology engineering in a networked world. Dordrecht: Springer; 2012. doi:10.1007/978-3-642-24794-1_1.

69. Villazón-Terrazas B, Vilches-Blázquez LM, Corcho O, Gómez-Pérez A. Methodological guidelines for publishing government linked data. In D. Wood, editor. Linking government data. New York: Springer; 2011, pp. 27–49. doi: 10.1007/978-1-4614-1767-5.

70. Santos C, Casanovas P, Rodriguez-Doncel V, Van der Torre L. Non-ontological Legal Resources Reuse and Reengineering, EKAW-2016, Workshop on the Semantic Web and Legal Knowledge, Bologna, November 2016.

71. Casanovas, P. Semantic Web Regulatory Models: Why Ethics Matter. Philosophy & Technology. 2015; 28(1):33–55

72. Casanovas P, Pagallo U, Palmirani M, Sartor G, editors. AI Approaches to the Complexity of Legal Systems IV. Social Intelligence, Models and Applications for Law and Justice Systems in the Semantic Web and Legal Reasoning, LNAI 8929, Heidelberg: Springer; 2014. doi:10.1007/978-3-662-45960-7

73. Boddington P. Big data, small talk: Lessons from the ethical practices of interpersonal communication for the Management of Biomedical big Data. In: Mittelstadt BD, Floridi L, editors. The ethics of biomedical data. Dordrecht: Springer; 2016. p. 277–305.

74. Walzer M. Liberalism and the art of separation. Political Theory. 1984;12(3):315–30.

75. Walzer M. Spheres of justice: a defense of pluralism. New York: Basic Books; 1983.

76. Nissenbaum, H. Privacy as contextual integrity. Wash. L. Rev.; 2004; 79:119–154.

77. Nissenbaum H. Privacy in context: technology, policy, and the integrity of social life: Stanford University Press; 2010.

78. Nissenbaum H. A contextual approach to privacy online. Daedalus. 2011;140(4):32–48.

79. Barth A., Datta A., Mitchell JC., Nissenbaum H. Privacy and contextual integrity: Framework and applications. In: 2006 I.E. Symposium on Security and Privacy, 21–24 May. Proceedings IEEE 2006. p. 15 pp.-198. doi:10.1109/SP.2006.32.

80. Floridi L. The Ethics of Information. Oxford: Oxford University Press.

81. Mittelstadt BD, Floridi L. The Ethics of Big Data: Current and foreseeable issues in biomedical contexts. In: Mittelstadt BD, Floridi L, editors. The Ethics of Biomedical Data. Dordrecht: Springer; 2016. p. 445–80.

82. Dwork C, Roth A. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science. 2014;9(3–4):211–407.

83. Simonite T. Apple's New Privacy Technology May Pressure Competitors to Better Protect Our Data, MIT Technology Review, August 3, 2016. Available at: https://www.technologyreview.com/s/602046/apples-new-privacy-technology-may-pressure-competitors-to-better-protect-our-data/?utm_campaign=content-distribution&utm_source=dlvr.it&utm_medium=twitter. Accesed 5 October 2016.

84. Gillespie T. The relevance of algorithms. Media technologies: Essays on communication, materiality, and society. T. Gillespie, P. Boczkowski, K. Foot, editors. Cambridge, MA: MIT Press Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.692.3942&rep=rep1&type=pdf. Accessed 18 October 2016.

85. Domingo-Ferrer J, Soria-Comas J, Ciobotaru O. Co-utility: Self-enforcing protocols without coordination mechanisms. In: Industrial Engineering and Operations Management (IEOM), 2015 International Conference, IEEE, 1–7. doi:10.1109/IEOM.2015.7093833

86. Koops B-J, Hoepman JH, Leenes R. Open-source intelligence and privacy by design. Computer Law & Security Review. 2013;29(6):676–88.

87. Casanovas P, Arraiza J, Melero F, González-Conejero J, Molcho G, Cuadros M. Fighting Organized Crime Through Open Source Intelligence: Regulatory Strategies of the CAPER Project. In: R. Hoekstra, editor, JURIX-2014, Legal Knowledge and Information Systems 271, Amsterdam: IOS Press; pp. 189–198. doi:10.3233/978-1-61499-468-8-189

88. Colesky M., Hoepman JH., Hillan C. A Critical Analysis of Privacy Design Strategies, Security and Privacy Workshops (SPW). 2016; IEEE. doi:10.1109/SPW.2016.23.s

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

90. Casanovas P. Open Source Intelligence, Open Social Intelligence and Privacy by Design. In: A. Herzig, E. Lorini, editors. Proceedings of European Conference on Social Intelligence (ECSI), Barcelona, November 3–5,2014; CEUR; 2014, vol. 1283, pp. 174–185. http://ceur-ws.org/Vol-1283/paper_24.pdf. Accessed 5 October 2016.

91. Klitou D. A solution, but not a panacea for defending privacy: the challenges, criticism and limitations of privacy by design. In: Preneel B, Ikonomou D, editors. Privacy technologies and policy, first Annual privacy forum, APF 2012, LNCS 8319. Berlin: Springer; 2012. pp. 86–110. doi:10.1007/978-3-642-54069-1_6.

92. Mendelson D, Wolf G. My electronic Health Record'Cui Bono (For Whose Benefit)? 24 Journal of Law and Medicine, 283. Available at: http://www.zorgictzorgen.nl/wp-content/uploads/2016/12/SSRN-id2881787.pdf. Accessed 17 February 2017.

93. Caldicott F. Review of data security, consent and opt-outs, National Data Guardian for Health and Care, 6 July 2016. Available at https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs. Accessed March 10 2017.s

94. BBC News, BBC News, US Healthcare records offered for sale online, 27 Jun3 2016. available at http://www.bbc.com/news/technology-36639981. Accessed March 10th 2017.

95. Fernández-Alemán JL, Carrión-Señor I, Oliver Lozoya PA, Toval A. Security and privacy in electronic health records: A systematic literature review. J Biomed Inform. 2013;46(3):541–62. doi:10.1016/j.jbi.2012.12.003.

96. Mahfuth A, Dhillon JS, Drus SM. A systematic review on data security and patient privacy issues in electronic medical records. Journal of Theoretical and Applied Information Technology. 2016;90,(2):106–115. Available at: http://www.jatit.org/volumes/Vol90No2/12Vol90No2.pdf [accessed 25 March 2017].

97. Rezaeibagha F, Win KT, Susilo W. A systematic literature review on security and privacy of electronic health record systems: technical perspectives. Health Information Management Journal. 2015;44(3):23–38. doi:10.12826/18333575.2015.0001.

98. Kun L, Beuscart R, Coatrieux G, Quantin ., with consultations and contributions from Robert. Mathews. Improving outcomes with interoperable EHRs and secure global health information infrastructure. In: Medical and Care Compunethics 5, L. Bos et al. (Eds.), Amsterdam: IOS Press, 2008, pp. 68–79.

99. Chalasani S, Jain P, Dhumal P, Moghimi H. Wickramasinghe. Content architecture applications in healthcare. Heal Technol. 2014;4(1):11–9. doi:10.1007/s12553-014-0075-x.

100. Sittig DF, Wright A. What makes an EHR "open" or interoperable? J Am Med Inform Assoc. 2015;22(5):1099–101. doi:10.1093/jamia/ocv060.

101. Mandel JC, Kreda DA, Mandl KD, Kohane IS, Ramoni RB. SMART on FHIR: A standards-based, interoperable apps platform for Electronic Health Records. Journal of the American Medical Informatics Association. Res Appl. doi:10.1093/jamia/ocv189.

102. Kindrick JD, Sauter JA, Matthews RS. Improving conformance and interoperability testing. StandardView. 1996;4(1):61–8.

103. Noyes H. Direct democracy as a legislative act. Chapman Law Review. 2016;19(1):199–218.

104. Schwrzschild M. Popular initiatives and American federalism, or Putting Direct Democracy in its Place. Journal of Contemporary Legal Issues. 2014;13:531.

105. DuVivier KK. The United States as a democratic ideal? International Lessons in Referendum Democracy Temple Law Review. 2006;79:821.

106. Kirby M. The Australian Republican Referendum 1999 - Ten Lessons, Law and Justice Foundation Available at: http://www.lawfoundation.net.au/ljf/app/&id=DF4206863AE3C52DCA2571A30082B3D5. Accessed 10 March 2017.

107. Hoffmann C. The 8 categories of crowdsourcing in Healthcare, MedCityNews, January 3 2015. Available at: http://medcitynews.com/2015/01/8-categories-crowdsourcing-healthcare/?rf=1. Accessed 15 October 2016.

108. Swan M. Health 2050: the realization of personalized medicine through crowdsourcing, the quantified self, and the participatory biocitizen. Journal of Personalized Medicine 2012; 2(3): 93–118. doi:10.3390/jpm2030093. Available at: http://www.mdpi.com/2075-4426/2/3/93/htm. Accessed 15 October 2016.

109. Ranard BL, Ha YP, Meisel ZF, Asch DA, Hill SS, Becker LB, Merchant RM. Crowdsourcing—Harnessing the masses to advance Health and Medicine, a systematic review. J Gen Intern Med. 2014;29(1):187–203.

110. Boulos MNK, Resch B, Crowley DN, Breslin JG, Sohn G, Burtner R, Chuang KYS. Crowdsourcing, citizen sensing and sensor web technologies for public and environmental Health surveillance and crisis management: Trends, OGC standards and application examples. Int J Health Geogr 2011;10(1): 1. Available at: http://ij-healthgeographics.biomedcentral.com/articles/10.1186/1476-072X-10-67. Accessed 15 October 2016.

111. Poblet M. editor. Mobile technologies for Conflict management: Online Dispute Resolution, Governance, Participation. Dordrecht: Springer, 2011. doi: 10.1007/978-94-007-1384-0

112. Poblet M, García-Cuesta E, Casanovas P. Crowdsourcing: Roles, Methods and Tools for Data-intensive Disaster Management. Information Systems Frontiers, published 12 January 2017. doi:10.1007/s10796-017-9734-6.

113. Cameron K. The 7 Laws of Identity, May 2005. Available at: https://msdn.microsoft.com/en-us/library/ms996456.aspx. Accessed 10 March 2017.

114. Garcia M, Grassi PA. NISTIR 8103. Advanced Identity Workshop on Applying Measurement Science in the Identity Ecosystem: Summary and Next Steps. Applied Cybersecurity Division Information Technology Laboratory, September 2016. Available at: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8103.pdf. Accessed March 10 2017.

115. Grassi PA, Nadeau EM, Galluzzo RJ, Dinh AT. NIST Internal Report 8112 (draft). Attribute Metadata, August, 2016.. Available at: https://pages.nist.gov/NISTIR-8112/. Accessed 10 March 2017.

116. Lessig L. Code and Other Laws of the Cyberspace, v.2.0. 2006. http://codev2.cc/. Accessed 15 October 2016.

117. Klitou D. Privacy-invading technologies and privacy by design. Berlin: Springer and TMC Asser Press; 2014. doi:10.1007/978-94-6265-026-8_2.

118. Hardy Q. The Web's Creator Looks to Reinvent It. New York Times, June 7 2016. Available at: https://www.nytimes.com/2016/06/08/technology/the-webs-creator-looks-to-reinvent-it.html?_r=2. Accessed 10 March 2017.

119. Manyika J, Lund S, Bughin J, Woetzel J, Stamenov K, Dhruv D. Digital globalization: The new era of global flows. Report. Mackinsey Global Institute. March 2016. Available at: http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows. Accessed 5 October 2016.

120. Kennedy B. Most Americans trust the military and scientists to act in the public's interest, FactTank, October 18, 2016. Available at: http://www.pewresearch.org/fact-tank/2016/10/18/most-americans-trust-the-military-and-scientists-to-act-in-the-publics-interest /. Accessed 20 October 2016.

121. C.L. Philip Chen, Zhang C-Y. Data-intensive applications, challenges, techniques and technologies: A survey on Big Data, Information Sciences;s 2014, 275: 314–347. doi:10.1016/j.ins.2014.01.015

122. Andrighetto G., Governatori G., Noriega P., van der Torre L., editors. Normative Multi-Agent Systems, Saarbrüucken/ /Wadern: Schloss-Dagstuhl Publishing, 2013. doi:10.4230/DFU.Vol4.12111.i. Available at: https://pdfs.semanticscholar.org/15be/bb5940263a609efef75df357bf33f82c1e26.pdf. Accessed 25 March 2017.

123. Mendelson G and Mendelson D. Criteria of Evaluation of Personal Injury and Damage in Australia. In: SD Ferrara, R Boscolo-Berto, G Viel, editors. Personal Injury and Damage Ascertainment under Civil Law. Dordrecht: Springer; 2017, pp. 467–507.