J Multidisciplinary Scientific Journal

MDPI

Article

Law, Socio-Legal Governance, the Internet of Things, and Industry 4.0: A Middle-Out/Inside-Out Approach

Pompeu Casanovas [1,2,*], Louis de Koker [1,3] and Mustafa Hashmi [1,2,4]

[1] La Trobe LawTech, La Trobe Law School, La Trobe University, Melbourne, VIC 3086, Australia; l.deKoker@latrobe.edu.au (L.d.K.); m.hashmi@latrobe.edu.au (M.H.)
[2] Institute of Law and Technology, Autonomous University of Barcelona (IDT-UAB), 08193 Bellaterra, Spain
[3] Department of Commercial and Labour Law, University of the Western Cape, Bellville, Cape Town 7535, South Africa
[4] School of Engineering, Information and Physical Sciences, Federation University, Brisbane, QLD 4000, Australia
* Correspondence: p.casanovasromeu@latrobe.edu.au; Tel.: +61-043-596928

Abstract: The Web of Data, the Internet of Things, and Industry 4.0 are converging, and society is challenged to ensure that appropriate regulatory responses can uphold the rule of law fairly and effectively in this emerging context. The challenge extends beyond merely submitting digital processes to the law. We contend that the 20th century notion of 'legal order' *alone* will not be suitable to produce the social order that the law should bring. The article explores the concepts of rule of law and of *legal governance* in digital and blockchain environments. We position legal governance from an empirical perspective, i.e., as an explanatory and validation concept to support the implementation of the rule of law in the new digital environments. As a novel contribution, this article (i) progresses some of the work done on the *metarule* of law and complements the SMART *middle-out approach* with an *inside-out approach* to digital regulatory systems and legal compliance models; (ii) sets the state-of-the-art and identifies the way to explain and validate legal information flows and hybrid agents' behaviour; (iii) describes a phenomenological and historical approach to legal and political forms; and (iv) shows the utility of separating *enabling* and *driving* regulatory systems.

Keywords: regulatory models; rule of law; metarule of law; Internet of Things; Industry 4.0; Web of Linked Data; Artificial Intelligence; legal compliance; legal professions

Citation: Casanovas, P.; de Koker, L.; Hashmi, M. Law, Socio-Legal Governance, the Internet of Things, and Industry 4.0: A Middle-Out/Inside-Out Approach. *J* **2022**, *5*, 64–91. https://doi.org/10.3390/j5010005

Academic Editor: Larisa Ivascu

Received: 3 December 2021
Accepted: 6 January 2022
Published: 21 January 2022

1. Introduction

This is a paper on the concept of *legal governance* and the convergence of technologies represented by the Web of Data (WoD), the Internet of Things (IoT), and Industry 4.0. Its point of departure is that the 20th century concept of 'legal order' *alone* will not be suitable to produce the social order that the law should bring. In practical terms, it holds that more laws and more regulations, standards, and regulators will not solve the challenge of legal governance in the IoT and Industry 4.0 environments. The convergence of complex technologies will change the context to be regulated as well as what should be regulated—the perception, processing, and emergence of a hybrid human–machine behaviour that is not only human or only computational. This behaviour is *in between and beyond* the 20th century human/machine divide. It will produce new kinds of actions and social outcomes that are not easily captured and regulated by the way we have conceived rules and norms in the past. It will also do so in volumes and at speed with far higher levels of complexity than had to be processed by the legal system in the past. This new reality is not augmented reality, it is an *emergent, added* reality to our lives and social interactions. This is a *hybrid* reality. How are we going to regulate it?

This paper considers the concept of *legal governance* and how it could be made meaningful and relevant to the new reality. We do not intend to change or challenge the normal

usage of well-established concepts in legal theory and the legal doctrine deploying the rule of law, such as 'legal system', 'legal order', 'enforcement', 'legal rule', 'legal norm', and the like[1]. These will continue to be used in the normal sense lawyers and legal scholars have adopted in the 20th century. This paper, however, introduces 'legal governance' from another perspective, from an empirical approach, i.e., as an explanatory and validation notion, primarily informed by a social and cognitive science perspective, to support the implementation of the rule of law in IoT and Industry 4.0 environments.

To delve into the complexity of legal governance, we resume in this article the conceptual work we have discussed in previous articles on big data and regulatory models (Casanovas et al. [1,2,3,4]; Hashmi et al. [5,6]; de Koker et al. [7]; Poblet et al. [8]; Governatori et al. [9]; Rodríguez-Doncel et al. [10,11]). We also link it to other concepts that we have previously analyzed to produce a holistic view of the regulatory domain, especially as applied in the regulatory toolbox set at *On Good AI Governance: 14 Priority Actions, a SMART Model of Governance, and a Regulatory Toolbox*, the AI4People Report on the legal side of governance [12]. However, the concept of legal governance was not made fully explicit in the latter report. Its meaning related to Artificial Intelligence (AI) was taken for granted. In essence, legal governance in the IoT and Industry 4.0 environments entails that (i) concepts such as 'enforcement', 'implementation', 'effectivity', 'application' and so forth, i.e., the concepts linked to the practical realization or performance of the law, and (ii) the concepts related to the system as a whole—for example, 'validity' or 'legality'—should be empirically defined and used to create a specific regulatory mindset and toolkit for the IoT. This allows metrics to be applied, offering in return more information about the system's ability to adapt to its environment, to create a new one, and to sustain legal ecosystems. For this approach, legal governance means socio-legal governance.

2. A Changing Regulatory Framework

2.1. Web 4.0, Industry 4.0, and IoT

Web 4.0 has been described as a 'symbiotic', 'intelligent', 'read-write-execution-concurrency' web [13] in between humans and machines, explicitly related to social computing [14] and the emergence of the IoT [15]. Industry 4.0 is a term first used at the Hanover Messe Fair in 2011 as *Industrie 4.0* and quickly adopted into English. It defines the relation of industrial workplaces and production with the IoT Cyber-Physical Systems (CPS) in relation to the industrial processes involved in manufacturing, engineering, material usage and supply chain and life cycle. Oztemel and Gursev [16] define the notion as a manufacturing philosophy that includes modern automation systems with an increasing level of autonomy, flexible and effective data exchanges enabling the implementation of next generation production technologies, and also being more personal and more agile in production as customized products.

Industry 4.0 has two key factors: *integration* and *interoperability* [17]. Drath and Horch [18] differentiate three CPS levels: the physical objects, data models of physical objects in a network infrastructure (cloud), and services based on the available data. Using the Strategic Options Development and Analysis (SODA) method, Almeida [19] has drawn a cognitive map with five dimensions: symbiotic, Web of Things, social computing, pervasive, and ubiquitous computing. Lee et al. [20] propose a five-level CPS architecture for developing and deploying a manufacturing application through a sequential workflow—smart connection, data-to-information conversion, cyber level (information hub, e.g., twin model for information and machines), cognition (decision-support system), and configuration (resilient control system). Papcun et al. [21] relate CPS with Human–Machine Interaction (HMI) 4.0 and emphasize that Service Oriented Architectures (SOA) for HMI should be built on robust (fault-tolerant) and quick (good latency) API (Application Programming Interface), because HMI has to react to alarms very quickly, and operators have to have up-to-date information about the production.

[1] Please note our use of single (') and double (") quotation marks in this paper. We use the former to individuate some terms, or concepts, as is the case in the example above (about 'legal systems', 'legal order' etc.). We use double quotation marks for literal quotations from other sources.

Based on a quantitative text analysis and a qualitative literature review, the survey by [22] identifies four design principles of Industry 4.0: *technical assistance* (virtual and physical), *interconnection* (collaboration, standards, and security), *information transparency* (data analytics and information provision), and *decentralized decisions*. Industry 4.0 can improve cross-organizational logistics in terms of real-time information flows and end-to-end supply chain transparency, helping companies to optimize value creation. For instance, Kanban—the system of supplying parts and materials just at the very moment they are needed in the factory production process—and *Just-in-Time/Just-in-Sequence* logistics can be drastically ameliorated [23]. The new discipline of Business and Information Systems Engineering (BISE) is focusing on these lifecycle changes based on the industrial integration of the IoT [24]. The Industry 4.0 convergence with Web 4.0 and the IoT is proceeding at pace, increasingly affecting society as a whole. The convergence gained momentum during the COVID-19 pandemic and accelerated its impact [25].

What should especially be noted is the fusion of technologies brought about by the Industry 4.0 revolution, which is blurring the lines between the physical, digital, and biological spheres, turning data into more manageable information, increasingly in the form of "*open data*" that can be freely used, reused, and redistributed by anyone. This is the essential point where the IoT, Web 4.0 and Industry 4.0 converge. What are the main issues? What are their regulatory requirements? We will explore these questions below.

2.2. New Regulatory Challenges

As expected, the convergence between Web 4.0, Industry 4.0, and the IoT (i) has already challenged the regulatory landscape, e.g., relating to law, governance, and the legal profession; (ii) brought about new regulatory challenges regarding, e.g., legal liability, data rights, data protection, trade restrictions, agreements, standards, contract models, supervision, surety, monitoring, and control; and (iii) created and stabilized new regulatory (or socio-legal) ecosystems that bind together all related stakeholders.

The IoT, for example, is changing the social nature, function, and perspective of regulatory systems, both in their public and private dimensions. Recent Gartner reports have highlighted that legacy silos of systems, data, and processes continue to limit government participation in broader digital ecosystems and constrain the implementation of fully digital end-to-end citizen services [26]. These results also reflect the evolution of the web from Web 3.0 to Web 4.0, the emergence of Industry 4.0, and the construction of regulatory ecosystems.

Open data can enable greater transparency, higher levels of citizen trust, better public service delivery, and more effective policy-making, but *opening up data does not mean having to make it public* [27]. Setting up platforms or apps for citizens' participation is not ensuring tangible results, it does not lead *per se* to reuse and value creation. Something else is needed, as the roles of citizens, consumers, stakeholders, and actors might be also changing in the new data-driven scenarios of the IoT.

From 2018 on, *Rules as Code*, a regulatory movement fostered by some government agencies, civil servants, and entrepreneurs in New Zealand, Australia, Canada, France, and some other countries, try to facilitate the enhancement of citizens' rights and a faster drafting and implementation of legal provisions by means of computer languages [28]. *Better Rules* and *Legislation as Code* are parallel developments as well (i) to design policies and (ii) to create and publish regulations, legislation, and policies as machine- and human-readable [29].

Gartner analysts, again, have recently represented the emerging trends in e-government into a new *2021 Hype Cycle for Digital Government Technology*[2]. However, the interpretation of the proposed solutions—digital twins and automated compliance by design—are somewhat surprising:

[2] Gartner Group: *Top Technology Trends in Government for 2021,* (Retrieved 20 November 2021 from https://www.gartner.com/en/doc/742950-top-technology-trends-in-government-for-2021).

> *A digital twin of a citizen is a digital representation of an individual. [. . .]. Governments are developing digital twins of citizens to monitor the environment citizens live in and address health, safety, travel, and social media impacts on society. The spectrum of complexity of the models and tools can help governments make better decisions for monitoring and supporting patients, prisoners, passengers, or the elderly. Some governments, such as China's, are building a scoring methodology. Aggregated citizen twins can help map broad patterns and drive resource allocation. [. . .] By implementing MRL (Machine-Readable Legislation), the room for interpretation of legislative or executive intent is eliminated from the process, instead making the law that is passed the same as that which is implemented*. [30]

However, assuming that "the policy is the technology and technology is the policy and the two are inseparable in a digital society", "closing the gap between legislative intent and implementation", and the crude projection of new technological trends to legislative and case-based law, are components of the problem, not of the solution. Doing so, the new *hybrid reality* we are trying to understand is completely set apart. The problem is not that these kinds of solutions are wrong. They are simply not helpful to address the challenges of the emergent reality that we are trying to understand, capture, and (hopefully) plot in design modeling.

We contend that only a holistic, relational view can appropriately address data-related hindrances, linking societal, economic, political, and legal dimensions to human-centered interactive computing. Machine-readable legislation (MRL) and legal Open Linked Data (LOD) have been developed for twenty years now (legalXML[3], legalRuleML[4], legal ontologies, see [11,31–33]) but their aim is not replacing human-driven institutions with corporate social engineering techniques[5].

Semantic Web researchers and developers have been sensitive to the social uses and impact of the technology they are building and deploying in social environments [35–38]. The present Semantic Web based on schema.org is used by more than 1.2 billion web pages hosting more than 38 billion semantic statements [39]. Surveys on the WoD literature based on a mixed methods approach—both qualitative (top-down) and data-driven (bottom-up) using PoolParty, Rexplore, and Saffron[6])—have already provided evidence that topics such as linked data, open data, and data sources have an upward trend, while topics such as semantic web, web services, service description and ontology matching appear to be on a downward trend [40]. IoT, sensor and streaming data are identified as future topics. The way how legal provisions will be executed in real time, and the way how knowledge graphs, MRL, and NLP techniques will be developed and used for the governance of the layered information flows occurring in Industry 4.0, are still being researched. As we will argue in the remaining sections below, the implementation of law as data, semantic reusability and scalability, legal knowledge graphs for compliance, and blockchain applications, are challenges that need the coordination and cooperation of all agents involved, artificial and human.

2.3. The Emergence of LawTech Web Services

In this regard, the emergence of LawTech web services aims to bring technological solutions and law to business, industry, and people, enabling them to better organise and automate both the management of their legal data and legal operations. *LawTech* is a

[3] OASIS legalXML specifications, (Retrieved 18 December 2021 from https://legalxml.wpengine.com/)

[4] OASIS LegalRuleML, (Retrieved 18 December 2021 from https://docs.oasis-open.org/legalruleml/legalruleml-core-spec/v1.0/legalruleml-core-spec-v1.0.html)

[5] Cf. the results of the 3rd COHUBICOL (Counting as a Human Being in the Era of Computational Law) Philosophers' Seminar organised by Mireille Hildebrandt and Laurence Diver on 'The Legal Effect of Code-driven Law' in November 2021, especially Palmirani [34] on this subject.

[6] Cf. Kirrane et al. [40]. *PoolParty* is a semantic technology suite that supports the creation and maintenance of thesauri by domain experts. *Rexplore* is an interactive environment for exploring scholarly data that leverages data mining, semantic technologies, and visual analytics techniques. *Saffron* is a topic and taxonomy extraction tool whose main applications include expert finding, document classification and search.

comprehensive notion that embraces the activities and solutions of a range of companies developing products to support the application of law and the functioning of legal professionals and the legal system, including the so-called *FinTech, RegTech, InsureTech*, and *SupTech* companies.

Over the past five years, an expanding legal market has formed around LawTech where companies offer a variety of legal services mainly based on AI and machine learning solutions—not just the more traditional e-discovery but supervision, monitoring and automatic compliance of regulatory systems, including smart contracts, cryptocurrencies and online dispute resolution [41,42]. Mills and Übergang [43] includes a non-complete list of companies already operating in the market, along with the fields of automation: (i) expert knowledge and compliance, (ii) legal research (interpretation and resolution of cases), (iii) prediction sentences and cases (legal analytics), (iv) electronic discovery (e-discovery), and (v) intelligent contracts (smart contracts). However, it still is a volatile market. According to Blijd [44] LawTech venture capital investments increased dramatically until January 2019. From 2015 to October 2019, 992 LawTech portals disappeared, but many others were created at the rate of 2.4 new start-ups per day. Blijd [44] reckoned 4298, with a support of $22.7 billion of venture capital. He calculated a 532% decline in February 2020 in LawTech venture capital funding. Losses have been confirmed at the end of the year because of the pandemic [45,46][7].

Recent ILTA surveys corroborate that law firms' interest in this market based on AI techniques is higher than ever [47–51]. Especially in the Asia-Pacific market, the offer of LawTech web services and legal analytics increases in part because the number of law firms is also growing [52]. In May 2020, without recovering yet, Blijd [46] has seen greater activity and a greater capital flow in ten areas that he as grouped by pairs: (i) divorces and real estate, (ii) lawsuits and litigation, (iii) fraud and identity, (iv) supplier chains and risk, and (v) accounting and spending. He also points to a greater organisation in what has started to be called CivicTech, the collective non-institutional organisation to solve social problems (such as the protection of victims of gender violence during the crisis). The numbers have skyrocketed with the pandemic. Some analysts (e.g., Blijd [53], based especially on S1 of INTAPP) estimate the combined market value of LawTech and GRC (Governance, Risk and Compliance) to be as high as US $3 trillion ($3 \times 10^{12}$)[8].

For purpose of this paper several aspects of the impact of the IoT technologies on legal practice highlighted by the recent literature are relevant to note: (i) legal entities on the web [9]—i.e. legal concepts—can be used not just for information retrieval but also enhanced for legal activities and operations (contracting, drafting, sentencing) combined with factual data flows; (ii) Machine Learning prediction power can lead to better and more nuanced decisions, increasing the need for structuring data, exercising judgments to triage options [55]; (iii) thus, as assessed by Tung [55] (quoting Schrage [56]), AI can supercharge management tools such as the Pareto principle beyond the 80/20 threshold to target 10%, 5% or even less than 1%[10]; (iv) robust predictions can generate more valuable and reliable insights (ibid.) and are stimulating the demand, as the examples of legal

[7] Blijd's estimation is based on Docusign, Legalzoll, Disco S-1, Intapp S-1, Docusign S-1, NUIX Prospectus, Law Society in relation to their registers *SEC filing* (*U.S. Securities and Exchange Commission*).

[8] Cf. Intapp S-1 [54] (p. 8) "We believe private capital, investment banking, legal, accounting, and consulting collectively represent a massive industry with $3 trillion in total global revenues, based on research we have conducted. We believe this industry has a significant need to utilise software to help drive business success, with total address-able market for business software at approximately $23.9 billion. We calculate our total addressable market by multiplying the number of firms in the professional and financial services industry by the potential annual contract value of the software solutions used in the business management of such firms, based upon our historical data and experience. We estimate the total number of firms across the private capital, investment banking, legal, accounting, and consulting sectors on a global basis to be approximately 60,000 firms. This figure excludes firms in the professional services industry with fewer than 50 employees, as they are outside of our current target market focus."

[9] The expression 'legal entities' refer to digital entities in relation to the representation languages of the web; this expression is not used here in the usual legal meaning (referred to persons).

[10] Pareto's principle claims that 80% of effects (sales, revenue, etc.) come from 20% of causes (products, employees, etc.) [56]. These correlations do not hold for the IoT: "Extreme distributions transcend and dominate industry.

analytics companies show in the last five years—Judicata, Neota Logic, Ross, among many others [43,57,58]; (v) the available technology is changing the relation between the legal profession and its clients (as users, consumers, citizens) because it is transforming their expectations—as Rule [59] has recently contended, technology is empowering people and changing their idea of justice; and (vi) accordingly, faster and wider Online Dispute Resolution(ODR) can be carried out by platforms that are not just offering mediation in all its variants but algorithm-related advice and decision-making, but "the introduction of algorithms and Big Data into the dispute resolution arena is hardly a one-way, positive-only development" [60] (p. 45). We will return to this point in the last section. Pros and cons of legal technology applications should be carefully balanced.

The IoT impact is also reaching what is known as 'legal knowledge' so far, both in legal doctrine and in legal theory, based on prescriptive, enforceable provisions. In Industry 4.0, the convergence between the IoT, WoD (LOD), and Industry 4.0 changes the way in which regulatory and normative systems are implemented. The emergence of Open Rights systems, agreement technologies and blockchain secured transactions is fuelling the development of a digitally based society and culture. This means that the enforcement of norms through the central authority of the nation states is balanced by the emergence of socio-legal ecosystems, acting in the inter-space created by and within this convergence [8].

2.4. Socio-Legal Ecosystems

Within the contexts of Web 2.0 and 3.0, semantic ecosystems were identified as relevant to data governance:

> *The Social Web is an ecosystem of participation, where value is created by the aggregation of many individual user contributions. The Semantic Web is an ecosystem of data, where value is created by the integration of structured data from many sources.* [61]

People are producers and costumers, machines are enablers (ibid.). On Web 4.0, value is created through the layers of the IoT—i.e., it is a *hybrid* system, an ecosystem of things, entities or twins that may have replicas in the physical world, plus agents (human and artificial). In the same vein, a (socio)-legal ecosystem of artificial/human agents, information processing, robots and data is created and stabilized when the social behaviour of autonomous and semi-autonomous agents can be embedded, implemented, monitored, and controlled within the computer design. Intelligent web services, socio-technical systems and especially artificial normative socio-cognitive systems share this ability to set social ecosystems, and eventually a community of users.

Ten years ago, Mazhelis et al. [62] defined an IoT business ecosystem "as a special type of business ecosystem which is comprised of the community of interacting companies and individuals along with their socio-economic environment, where the companies are competing and cooperating by utilizing a common set of core assets related to the interconnection of the physical world of things with the virtual world of Internet." Three key technical domains were typically targeted: (i) *device* (sensing/actuating technologies), (ii) *connectivity* (providing the access and core network connectivity), (iii) and *application* services. The authors also identified some of the IoT regulatory roles: (i) Intellectual property rights (IPR) holder, (ii) standard development organization (SDO) (official organizations, industrial alliances, special interest groups focusing on standard development), (iii) regulatory bodies (controlling processes, as mandated by a legislative body), and (iv) legislative bodies.

From a legal viewpoint, fundamental questions and principles related to obligations/responsibilities, and liability/rights/accountability remain valid [63]. IoT ecosystems on the WoD involve different types of contracts, licenses, insurances, patents, privacy, and consumer and data protection (see, for the European framework [10], on NLP for legal services, [64]). However, the traditional legal approach will not be enough as the

Fewer than 10% of drinkers, for example, account for over half the hard liquor sold. Even more extreme, less than 0.25% of mobile gamers are responsible for half of all in-game revenue" [56].

complexity of the systems develop. In the case of extended vehicles and autonomous cars, competition law, for example, can only partially solve some of the issues that arise on data portability and access rights [65]. The civilian use of drones, unmanned aerial systems, and autonomous vehicles require enriched regulatory systems to implement security and privacy principles [66–68]. Smart cities are natural environments for linked open data [35,69] and this will give rise to legal questions at frequency and volume that the traditional legal approach cannot process and adjudicate.

A governance response to the evolution of the IoT requires a more granular regulatory approach [4]. A few years ago, big data ecosystems (BDEs) were viewed lacking the kind of metadata management support that was essential in traditional enterprise systems [70]. The challenges included (i) frequent evolution of both data sources and processing algorithms, (ii) need to share both data and algorithms, and (iii) analysis over long time periods (ibid.). Drafters and regulators have been focusing on these challenges to develop the digital EU market strategy [33]. The notion of IoT *legal governance* related to linked open data and forms of sustainable ecosystems has drawn much attention. The notion of *linked democracy* has joined the more familiar concepts of deliberative and epistemic democracy [8]. Data Ecosystems (DE) shape the next-generation smart environments [71] for Open Government Data Ecosystems (OGDE) [72–75].

Zuiderwijk et al. [76] (pp. 29–30) suggested a number of actions to build Open Data (OD) ecosystems. An OD ecosystem consists of a multilayered and plural framework "characterized by multiple inter-dependent socio-technical levels, dimensions, actors (including data providers, infomediaries, and users), elements and components", and a "need to address challenges related to policy, licenses, technology, financing, organization, culture, and legal frameworks and are influenced by ICT infrastructures". They systematically describe the activities that can be performed in the open data process, and elements of OD ecosystems that can be used to enable and support these activities. A lifecycle of data includes actions such as data creation, publication, exportation, importation, use, transformation and reuse. They offer a useful summary:

> *To create an open data ecosystem at least four key elements should be captured: (1) releasing and publishing open data on the internet; (2) searching, finding, evaluating and viewing data and their related licenses; (3) cleansing, analyzing, enriching, combining, linking, and visualizing data; and (4) interpreting and discussing data and providing feedback to the data provider and other stakeholders. Furthermore, to integrate the ecosystem elements and to let them act as an integrated whole, there should be three additional elements: (5) user pathways showing directions for how open data can be used, (6) a quality management system, and (7) different types of metadata to be able to connect the elements.* [76] (p. 17)

Linked data should be understood as integrating the IoT ecosystems as well, as "connectivity and smart components become more important than the physical element of the '*thing*'". A survey by Leminen et al. [77] on IoT and business models has shown that value drivers are related to the reduction of the real world–virtual world transaction costs, the reduction of operating costs, and the streamline of companies through heterarchical strategies. They differentiate two kinds of ecosystems: in a *hierarchy*, each node is connected to one parent node, whereas in a heterarchy, a node can be connected to any of its surrounding nodes without the need to go through or get permission from another node. Thus, "a *heterarchy* implies a relationship of interdependence and trust, and it is a complex and effective adaptive system, self-organised by a variety of non-hierarchical principles" [77] (p. 755). As we will contend later, trust is a very important element, not only for business models to thrive but to regulate the entire ecosystem and to relate it with broader regulatory environments. The idea of *heterarchy* is an important one, because it may help to better understand why the concept of legal governance can be useful to take IoT decentralised architectures into account.

Several proposals have been made in relation to decentralized architectures. Dasgupta et al. [78], for example, consider that decentralized IoT architectures like fog, cloudlets,

and edge have shown that centralized approaches to governance are not viable and consider IoT governance as an extension of IT governance through a 4I model framework: *Identify, Insulate, Inspect, and Improve*. Zdravković et al. [79] state that IoT ecosystems demands appropriate policy principles addressing M2M connectivity leaning on five categories: (i) *connectivity*, (ii) *privacy*, (iii) *security*, (iv) *standardization*, and (v) *data ownership*. Singh et al. [80] have convincingly argued that it is the exchange of information—the flow of data—that determines what happens in the IoT, and that a legal focus on transparency should be on communicating known risks and incentivising effective processes for identifying unknown risks. Thus, data-flow management and emerging data provenance methods that track the flow of data end to end should be developed to ensure compliance and transparent and accountable processes. Singh et al. [81] have also developed a perspective in which a middleware-enforced, unified policy model applies end-to-end, throughout the IoT chains of data flows.

Compliance with policy and regulatory models has been the subject of legal compliance developments, which for more than a decade now have extended business compliance models to social and legal environments using many different business languages and methodologies [6,82–84]. However, validation processes in this kind of layered architecture in the new IoT environments must still be developed. Legal compliance will be a key topic, as the whole information lifecycle should be designed and monitored to foster trust, transparency and accountability in a sequential, controlled process to deliver outcomes deemed as 'valid' or 'legal' *by* or *through design*. Trust is not necessarily a direct product of compliance, but it is a by-product of the conditions created by a sustainable legal ecosystem. In the IoT, we define trust as knowledge-based reliance on received information, that is, "an agent (i.e., a person or a software program) decides to trust (or not) based solely on her/his knowledge, and the decision to trust implies the decision to rely on the truth of received or on already known information to perform some action" [85] (p. 8). Thus, trust it is an essential component of the sustainability of legal ecosystems as will be shown later, but unlike reliability and legal compliance it is not a *continuum*, but a discrete category.

Blockchain technologies have already been incorporated into the compliance process [86,87]. In regard to legal compliance, *Compliance through Design* (CtD) will be decomposed from different approaches to select several implementation types according to the normative environment, selected formal languages, stakeholders, and the kind of processes to be regulated (regulatory compliance, legal compliance, partial compliance, full compliance, distributed compliance, etc.) [1–3,5,6,80,81,88]. Embedding compliance modeling into socio-legal ecosystems—with human and artificial agents—is the next step.

3. Socio-Legal Governance

3.1. Legal Governance and the Limits of Legal Instruments

The concept of legal governance, as such, is not new. It has been employed in several fields of social science with different meanings. To begin with, some usages of the term lean on the notion of governance, separating corporate governance from legal governance based primarily on statutory and case-based law. This is a common practice, meaning simply that legal implementation has different features. Other usages of the term highlight its practical side, referring to regulatory practices or models driven by Civil or Common Law-based policies. For example, the Law and Development Movement first pointed to the transplants of the rule of law to foster economic development in Latin America, Africa, and Asia. This movement has received critical attention from Law and Society authors since its inception in the late sixties of the past century [89,90]. Their work focused on the World Bank's concept of 'legal governance' meaning governance through the rule of law and procedural justice mechanisms to offer legal defenses and guarantees to small companies and entrepreneurs. Likewise, the term has been used in a similar way—"reactive law enforcement by courts and proactive law enforcement by regulators"—by financial scholars targeting suitable means to develop stock markets in transition economies [91].

Despite the socio-political differences of these authors, a common argument that they advance is the insufficiency of legal instruments to produce the intended economic and social effects. The same reasoning is evident in the work of the proponents of the legal origins thesis—discussing the economic value of the *Continental* rule of law vs. its *Common Law* counterpart (La Porta et al. [92] and the reply by Michaels [93])—and in some of the discussions around blockchain regulation through decentralized ledgers.

Hildebrandt's research (COHUBICOL)[11] distinguishes between artificial legal intelligence or data-driven law, based on machine learning; and cryptographic or code-driven law, based on blockchain technologies. Or, broadly, between two types of algorithmic regulation, *data-driven* and *code-driven* [94]. We should also distinguish between *smart contracts* and *blockchain technologies*. The first were developed before, self-executing contracts directly written into lines of code [95], and supported by Ethereum much later, in 2014. As it is well-known by now, blockchain is a distributed database that is shared among the nodes of a computer network, mainly used in cryptocurrencies systems to secure a decentralized record of transactions. It is designed to foster *trust* in a 'trustless' environment.

De Filippi et al. [96] and De Filippi [97] have argued that blockchain technology was created as a response to the 2008 financial crisis. Bitcoin and other blockchain-based systems were presented as an alternative to centres of traditional power such as financial institutions, banks, and even governments. It is contended that (i) blockchain relies on cryptographic rules to increase confidence in the operations of a computational system, (ii) this ultimately relies on the proper operation and governance of the underlying blockchain-based network, (iii) which require trusting a variety of actors to ensure the proper operation and governance of that underlying blockchain-based network. However, an important point is that it facilitates the creation of autonomous systems that can challenge the authority of governments and "what makes the technology particularly potent is its ability to facilitate the creation of resilient, tamper-resistant, and automated code-based systems that operate globally, providing people with new financial contractual tools that could replace key societal functions" [98]. This is the *lex cryptographia* without intermediaries with which people can construct an "order without law and implement what can be thought as private regulatory frameworks" (ibid.).

However, permissionless blockchains are distributed, decentralized peer-to-peer networks in which everyone can participate interacting with unknown counterparties, trusted or not. Citizens' rights constitute a challenge for blockchain technologies under the European law (e.g., subject's right to erasure and right to restriction of processing). This has been raising many concerns, as the clear allocation of responsibilities that is required by GDPR is not present in this situation [99]. Many solutions have been proposed, for instance, *polycentric governance* (*ex ante* execution and *ex-post* verifiability) [97], *aligning contracts* with doctrinal and judicial interpretation (through declarative rather than imperative languages) [100], *hashing* (the insertion of data in the blockchain) to offer public services [101,102], appropriate agreements between regulators and the private sector, and the elaboration of codes of conduct and certification mechanisms for blockchain technologies that should be "compliant by design" [99]. To the best of our knowledge, this has not been yet solved, but it shows that solutions are not based on legal instruments (national or international) *only* but mainly on the building of legal governance frameworks.

3.2. Phenomenology and Political History

Another legal governance example of interest is found in political history. The concept has been used in this context to point out the transformation of law and the state at the end of the 20th century in relation to the change in mindset fostered by economic globalization and privatization. "In contrast to conventional forms of institutional government, governance is a series of informal, flexible and expedient strategies of problem-solving and crisis

[11] COHUBICOL, (Retrieved 12 November 2021 from https://www.cohubicol.com/about/philosophers-seminar-2021/).

management based on bargaining and negotiation" [103] (p. 325). Legal governance in this context is the concept used to describe (i) the restructuring and replacement of the classic Weberian substantive and formal notion of law with a set of business, management-driven techniques of government, and (ii) the emergence of informal networks as *sites of governance* that "by definition, cannot be held accountable to elected, appointed or otherwise legitimate structures of authority" (ibid, 326). This type of analysis assumes a historical perspective in which organizational and rational forms of government are intimately related. According to it, the liberal 'legal formalism' of the rule of law, understood as a set of legal norms conceived as general, clear, public, prospective, and stable, was superseded at the beginning of the 20th century by alternative state-centered conceptions, according to which a substantive legal rationality was designed to concretize the application of law to the solution of specific social and economic problems.

Then, in turn, the economic, cultural, and political globalization that took place in the last twenty years of the past century changed the general framework again. In short,

> *while 19th century formal legal rationality was largely bracketed and superseded by the substantive rationality of the 20th-century regulatory state, both are now being challenged by the rise of a new legal rationality, namely, negotiated process rationality and the attraction it holds for the interests of corporate and transnational governance.* [ibid., p. 327]

This framework, sketched with broad strokes, is representative of political philosophy views rooted in the Hegelian, Marxist, or Frankfurt School analysis. It is not very granular, and its interpretation of what regulatory systems entail can be challenged. For example, the definition of substantive rule of law linked to rationality does not correspond to the regular legal one, in which the protection of civil or fundamental rights is deemed to play an essential role [104]. However, such a general framework holds some analytical benefits, and ignoring the warnings against equating corporate and government regulatory practices shared by many political scientists from (very) different backgrounds would not be a good strategy. We refer to Arendt (on automation, from 1951–1956, Simbirski [105]), Pitkin [106] (on political representation), Habermas [107] (on regulatory structures), Sassen [108] (on nationalism and territoriality) and Scheuerman [109] (criticising the 'affinity' between global economics and the rule of law).

Heidebrand's criticism is addressed both to the instrumental and the idealistic sides of the rule of law [110]. For a socio-legal governance formula, it is our contention that we can benefit from the historical-phenomenological perspective, retaining the formal scaffolding of the substantive rule of law without the need to reproduce its heavily overloaded historical interpretation.

In addition to the blockchain, another relevant example of reactive behaviour to an external crisis or a tough environment can be found in the corporate legal and compliance risk management sphere. In response to a spate of US financial scandals (e.g., Enron Corporation, Tyco International Plc, and WorldCom), the US Congress enacted the Sarbanes-Oxley (SOX)[12] Act in July 2002. The main objective of the SOX Act was to protect investors from fraudulent reporting by corporations by increasing management responsibility for the accuracy and comprehensiveness of corporate financial statements of large companies. This Act fueled business and corporate compliance developments to avoid fines and loss of reputation. Regulatory and corporate responses informed increased regulatory requirements for enhanced corporate compliance risk management, especially in response to international standards such as the Basel III[13] international regulatory framework for banks

[12] United States Public Company Accounting Reforms and Investor Protection Act (Sarbanes-Oxley Act) 2002, Public Law 107–204, 116 Stat. 745.

[13] Basel Committee on Banking Supervision (BCBS). Basel III: The Liquidity Coverage Ratio and Liquidity Risk Monitoring Tools, 2003, (Retrieved 16 December 2021 from http://www.bis.org/publ/bcbs238.pdf).

and Financial Action Task Force's international anti-money laundering and combating the financing of terrorism and proliferation standards[14].

These developments fueled interest in *compliance by design* initiatives to improve corporate compliance levels. Well-known corporate risk management models—such as the COBIT framework for information and related technologies (COBIT 5), in 2012)[15] and the (COSO) frameworks on internal control, risk management, governance and fraud deterrence—also incorporated legal (and ethical) requirements as essential elements for good corporate risk management.

Similarly, Section 18 of ISO/IEC 27002[16] on information security addresses compliance with legal requirements. In these frameworks and standards, however, 'legal governance' was not considered in its legal dimension, i.e., from a public space or civil rights approach, but rather from an internal corporate perspective, as components and necessary conditions of safe and successful business strategies that comply with complex regulatory requirements.

"Efficiency means doing something at the lowest possible cost and effectiveness means doing the right thing to create the greatest value for the company. In this context, IT operations must be carried out efficiently minimising security risks and in accordance with legal requirements" [112] (p. 75). This is known as '*IT governance*', developed in the first decade of the century as a set of responsibilities of corporate governance boards, and expanded in the second decade to audit, control, and monitor agencies and administrations in the public sector [113–115].

IT governance developments have fostered human rights activism and the reflection on ethics and the reconstruction of the public space. Even without a special political aim in mind, it seems reasonable that platform-driven economy, blockchain and the social and societal effects of the corporatization of public administrations should be submitted to public scrutiny and accountability before taxpayers, i.e., consumers and citizens. As advanced by de Filippi [96]—see also Hildebrandt [94]—there is a still unresolved tension between cryptocurrencies practices and investments and the way how they should become publicly accountable. Ethics might certainly play a role in the "uneasy co-existence" between "code as law and law as code" [116]. Floridi and Cowls [117] have suggested to simplify the ethical principles to be applied to AI building a framework with four classical core-principles—beneficence, non-maleficence, autonomy, and justice—and a new one that is relevant for our discussion: *Explicability*, "understood as incorporating both the epistemological sense of intelligibility (as an answer to the question 'how does it work?') and in the ethical sense of accountability (as an answer to the question: 'who is responsible for the way it works?" [117] (p. 1).

'Explicability' is not a synonym of 'explainability' (a more common concept in the field). In our understanding, the normative effects (responsibility/liability) endorsed by the former notion are not necessarily entailed by the latter. The model of meta-rule of law that will be briefly described in the next Sections could be understood from this point of view as well.

3.3. Rule and Metarule of Law

The rule of law refers to the principle that the law applies to everyone, in contrast to the idea that the ruler is above the law. In its classical formulation, it excludes tyranny (and its contemporary version, dictatorship), as it encompasses the creation of participatory political forms that put aside the passive role of the regulated, i.e., to some extent, rather than simply obeying, people subject to the regulations have to accept, acquiesce or even

[14] Financial Action Task Force (FATF), (Retrieved 16 December 2021 from https://www.fatf-gafi.org/home/).

[15] COBIT 5 identifies five basic principles, seven categories of enablers to govern and manage the information requirements, new process reference model, improved goals and metrics, and aligns with the (ISO/IEC 15504) process capability assessment model and (ISO/IEC 38500) Corporate governance of information technology [111].

[16] The ISO/IEC standard was revised in 2005, and renumbered (ISO/IEC 27002) in 2007. It was revised again in 2013, and in 2015 the (ISO/IEC 27017) was created to suggest additional security controls for the cloud which were not completely defined in (ISO/IEC 27002).

approve them formally through their cooperative behaviour. Thus, from a procedural point of view, the rule of law purports to restrict the arbitrary exercise of power, i.e., to avoid tyranny and dictatorship, as a political form. This poses the issue of legitimacy as a necessary (non-sufficient) condition for the existence of the rule of law.

In a more substantive definition, the rule of law refers to principles embracing fundamental rights. It broadly points to a regulatory framework protecting life, property, and—after the Enlightenment—the well-being of individuals, communities, and society as a whole. Negative rights, conceived as a shield to safeguard individuals from discretionary power, can be taken back to Medieval constitutionalism[17]. Positive rights, as enablers of social services and benefits (health, labor, housing…) are related to the development of Human Rights and political Constitutions in the last two centuries.

However, there is no single agreed definition of rule of law. Common law countries —including USA, Canada Australia, UK and most countries of the Commonwealth —understand the rule of law from a bottom-up approach, meaning the set of layered practices and behaviours that shape the production, management, and preservation of the legal order, centered on the case-based law carried out by Courts of Justice. Civil law countries—most European countries, France, Germany, Italy, Spain, etc.—understand it from a top-down approach, centered on the sovereignty of the nation-state, and setting a hierarchical rank for the generation of legal provisions and instruments of authorities of different kinds—Parliament, Government, Courts, and central, regional and local administrations. This specific organization of power was known in the 20th century as *Rechtstaat, état de droit, stato di diritto, estado de derecho*….

These nuances matter because modeling Human rights and the rule of law is based on functional requirements that lean on cultural and political assumptions that should be made explicit (according to the nature, objective, scope, and territory of regulations). Some law is also international and, especially as a result of economic and cultural globalization in the late 20th and early 21st centuries, transnational. Thus, one of the main challenges is implementing and extending the protections and provisions of the rule of law not only within the jurisdictional space of the nation-state but beyond, within the intersectional space of global business, industries, emergent markets, and geopolitical stakeholders. This transnational scope is one of the first features of the meta-rule of law that we will define later, *beyond* the rule of law applied to national states. The Greek particle *meta* [$\mu\varepsilon\tau\alpha$] means 'beyond' and 'above'. 'Metarule' usually means a rule governing other rules. But as in 'physics' and 'metaphysics' or 'data' and 'metadata', our use of 'meta' does not match the computational sense of 'on' or 'above'. As noted by the Merriam-Webster Dictionary, 'meta' "means '*transcending*' and is often used to describe a new but related discipline designed to deal critically with the original one "[18]. These are the concepts we have in mind when we use the term "metarule of law". The primary meaning of the metarule of law entails transcending the rule of law, extending its protections outside of the sovereignty of the nation-states avoiding its limitations. As we will see, this position is an opportunity to add this regulatory dimension to Linked Open Data (LOD). Thus, building it as a legal *open public* space as well.

It is worth noting that our aim is setting a suitable framework to validate the regulatory models to be applied in IoT, LOD, WoD and Industry 4.0 environments, platforms, and applications, from a legal point of view, i.e., embedding the protections of the substantive rule of law into the systems. There are three dimensions that should be built to perform the suite of tasks that are needed to carry it out: *social, legal, and technical*. The technological side imply the elaboration of a conceptual toolkit, including the use of algorithms, semantic languages, logic, and metrics to test and validate the models. As we will explain later, this technical dimension has a mediating role between (i) social descriptions, explanations,

[17] Cf. Art. 39 Carta Magna (1215). *No freemen shall be taken or imprisoned or disseized or exiled or in any way destroyed, nor will we go upon him nor send upon him, except by the lawful judgment of his peers or by the law of the land.*

[18] —a meaning apparently embraced by Facebook when it re-branded as Meta and launched its "metaverse" in 2021, (Retrieved 18 December 2021 from https://www.merriam-webster.com/dictionary/metadata).

and social data, and (ii) the legal normative provisions usually understood as sources of law (in the broad sense, including the four clusters we will describe in the next section, standards, protocols, values, etc.).

From this empirical approach, there are many problems to be solved at the methodological level (metrics, thresholds, triage of formal languages, modeling of causal chains, etc.). The elements of the theoretical discourse—'norm', rule', 'regulatory system', and the like—will be understood in context, i.e., cognitively *situated*, as our aim is setting the conditions to generate legal ecosystems. The ontological and epistemological levels will be set apart.

Stemming from the globalization process that occurred in the last decade of the past century, there is a rich tradition in legal philosophy and socio-legal scholarship focusing on regulations and the rule of law. Researchers stressed the difference between legal and regulatory systems as developed by business and corporative organizations, and how this would affect administrations and governments [118,119]. There is a continuous thread from "responsive law" [120], "responsive regulations" [118] to "really responsive regulations" [119], and "regulation theory" [121] that shapes the way how socio-legal scholars are facing the emergence of LawTech, RegTech and the increasing implementation of AI techniques to the legal fields. There is a divide as well that should be bridged with the way how AI & Law and semantic scholars build formal regulatory and normative systems [11]. Socio-legal scholars have pointed internally at the social dimension of regulations and externally at the dimension of technology so far. The other way around, AI & Law scholars have been internally focusing on the technical construction of models and externally on their social impact. We will propose a *middle-out* and *inside-out* approach in the next sections, as it is not possible building reusable and scalable solutions without formalization, just as it is not possible either to implement them without social theory.

Which legal governance models should apply to regulatory technologies in new socio-technical ecosystems, how should these governance models be implemented, and how could these toolkits encompass the general principles and protections of the rule of law?

3.4. Scheme of the Metarule of law

Figure 1 provides a general schematic representation of the rule of law, i.e., the principle that the ruler and the ruled are bound by the law. It highlights the difference between regulations that were conceived to rule human social behaviour, and the new digital dimension in which rules, principles, and instruments are embedded into formal languages and computational codes to be digitally generated, interpreted, and implemented. We should stress that, for us, this is a useful scaffolding to start building validation and causal models, but it is not a meta-model, as we presented it in [8].

Figure 1 contains two axes along the vertical binding power, i.e., the capacity of enforcing norms, and the horizontal social dialogue, i.e., the individual and collective behavioral expectations that bind members of society to each other. We will put aside here the problem of sovereignty, i.e. the foundations of power and authority[19]. The scheme of Figure 1 is flexible enough to allow different degrees and types of authority and power, and different political forms under the rule of law, excluding dictatorship and authoritarian regimes. It embraces (vertically) different forms of legitimate power, legal monism, legal pluralism and nation state polyarchies, under the condition of the active cooperation of the regulated (social dialogue, social power). Community and societal power are situated on this horizontal axis. This is not new: these two axes have been drawn in different ways by

[19] For a recent systematization, Pohle and Thiel [122], "…The issue is no longer *cyber sovereignty* as a non-territorial challenge to sovereignty that is specific to the virtual realm of the internet. Today, *digital sovereignty* has become a much more encompassing concept, addressing not only issues of internet communication and connection but also the much wider digital transformation of societies. Digital sovereignty is—especially in Europe—now often used as a shorthand for an ordered, value-driven, regulated and therefore reasonable and secure digital sphere." [Ibid. p. 13], see also Floridi [123] advocating for an European "differentiated integration".

many classical scholars (from Max Weber to Jürgen Habermas[20] and Elinor Ostrom[21]), and many legal and socio-legal scholars, e.g., Tuori [127], have been using them to situate rights and duties with regards to norms and the binding power of authorities (be they political, such as the state, or social, e.g., dominant social groups).

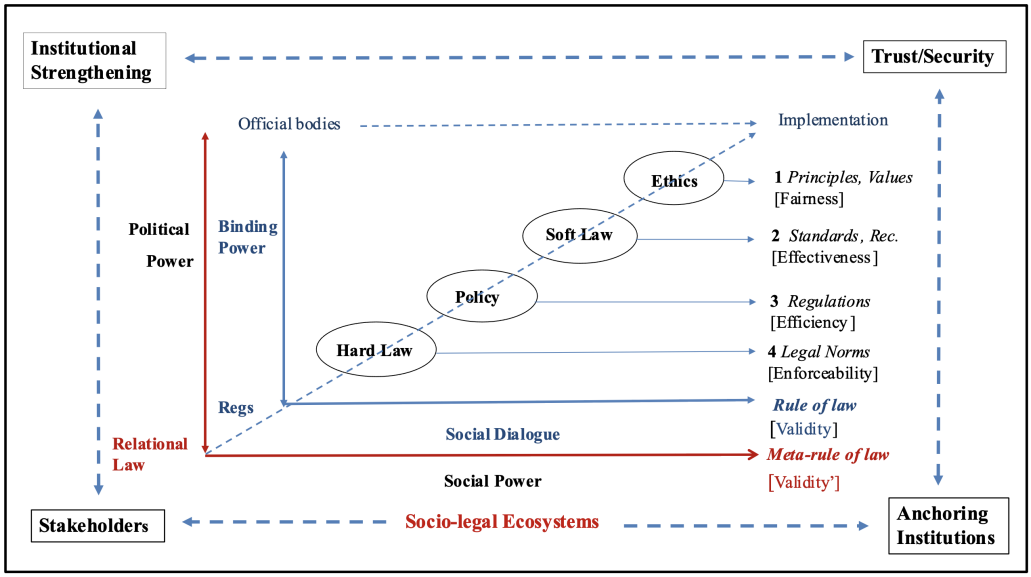

Figure 1. A general scheme for the meta-rule of law (Source: Poblet et al. [8]).

Thus, legitimation is deemed to be a component of legality, for 'what it counts as legal', emerges from the different degrees of adherence of the regulated, and the collective acceptance of the legal system, i.e., 'legality' can be considered a collective property that does not occur outside of the active social behaviour of all stakeholders in their different roles (consumers, citizens, tax-payers etc.). This is perfectly compatible and can be aligned with some definitions and principles set by specialised international institutions, e.g., according to the World Justice Project "the rule of law is a durable system of laws, institutions, norms, and community commitment that delivers: Accountability, Just Law, Open Government, and Accessible and Accountable Justice"[22].

Note that axes are a simple lineal way to represent the contrast between coercive power and negotiated dialogue, or binding vs. reciprocal relationships. However, in our version of the model there are three (not only two) dimensions that help interpreting this scheme and allow the emergence of regulatory ecosystems—the *social*, *legal*, and *linguistic* dimensions of the environment. Obligations and what is felt as being permitted or forbidden (i) occur in between these two axes and three dimensions, (ii) are formulated, expressed and communicated through natural and artificial languages.

In Figure 1, (i) *Hard law*, refers to legally binding obligations, either in the national or international fields, under regulations that can lead to adjudication court processes; (ii) *Soft law* consists of legally non-binding rules, best practices, protocols, standards and principles

[20] Habermas explicitly allocated rights in the horizontal axis as with "the conceptual move from the horizontal association of consociates who reciprocally accord rights to one another to the vertical organisation of citizens within the state" institutionalises the practice of self-determination" [107] (p. 135). In the Postscript he wrote two years later, he insisted on the social powers of the law, "a 'transmission belt' that picks up familiar structures of mutual recognition familiar from face-to-face interactions and transmits these, in an abstract but binding form, to the anonymous, systemically mediated interactions among strangers" [124].

[21] As it is well known by now, Ostrom [125] prioritised the organisation of community relationships at scale, as "the living units exist on a horizontal plane, however, rather than in vertical relationships to one another" [125] (p. 1074). However, in our complex world, Ostrom [126] also asserted that interaction effects often occur among variables at one or more tiers. "Thus, one needs to examine both vertical and horizontal relationships of a partially decomposable conceptual map" [126] (p. 11).

[22] cf. "What is the Rule of Law?", (Retrieved 16 December 2021 from https://worldjusticeproject.org/about-us/overview/what-rule-law).

that facilitate the governance of networks, organizations, companies, and institutions; (iii) *Policy*, which usually defines a (binding) plan that has been officially agreed by a business organization, a corporation or a government agency; and finally (iv) *Ethics*, which primarily refer to morals, social mores, values and principles that can infuse ethical codes and professional practices, and can also be incorporated into laws, policies, standards, best practices, and governance structures. These are regular components of the rule of law as they can be combined and embedded into formal languages and regulatory systems.

Principles are applied to and by agents, who often have specific roles in the regulatory ecosystem. For example, supervisory agencies typically monitor and control the policies laid down by governments to implement Acts and Regulations. They typically have the option to enforce fines after a violation of policy rules has occurred. Soft law instruments, i.e., non-binding standards and principles, are an increasingly important regulatory mechanisms. For instance, regarding the GDPR, the recent proposal for a European Digital Act[23] sets out risk analysis, intermediary services, and certification for AI products as a preferable regulatory strategy. Certifications of compliance can be obtained from an accredited certification body, but personal intermediaries are also considered in a low intensity non-compulsory strategy[24].

The semi-automation of legal governance is the next step, i.e., the creation of a regulatory interspace, bringing together all relevant stakeholders (including rulers, industry, and citizens), and the AI and legal instruments at their disposal. In this sense, the notion of *metarule* of law has been used both as a name and as a concept, much as the notion of rule of law, to design (i) the use of languages for legal and logical compliance expressing the concepts of rights, duties, obligations and prohibitions; (ii) AI instruments (such as machine and deep learning); (iii) semantic devices (NLP technologies, legal ontologies and ontology design patterns); and (iv) IoT technologies (augmented reality and digital twins), that are put in place to embed the negative and positive rights of the classic rule of law into platforms, websites, mobiles, and multi-agent and techno-social systems [128]. Substantial and formal (procedural) rights remain essentially the same, with some additions such as digital accessibility rights[25], but the fabric to enhance them—conceptualisations, contexts, environments, scenarios…—has dramatically changed.

Therefore, artificial languages and devices are regulatory components that mediate and bridge the content of norms, the legal institutions that are supporting them, and the subjects that must comply with them. Poblet et al. [8] put forward some ideas in the pursuit of distributed, technology-supported collective decision-making processes from a polycentric perspective. Thus, embedding/implementing the principles of the substantive rule of law into automated regulatory systems can foster the emergence of socio-legal ecosystems that are sustained and developed both by humans and machines in an intertwined way. The metarule of law refers to principles governing humans and programs, rights and languages, etc., to generate trust among officers and stakeholders of rights (in a multi-stakeholder digital governance process). The creation of socio-legal ecosystems refers to the social, formal, and legal conditions that are required to enhance these rights online in real time in WoD and IoT environments.

Rights, agency, and the coordination of artificial and human behaviour (M2M, M2H, H2M, M2H) lie at the core of the metarule of law. There are several ways to handle these issues and to offer a general governance framework. The notions of data and metadata,

[23] Brussels, 25.11.2020 COM(2020) 767 final 2020/0340 (COD) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European data governance (Data Governance Act), (Retrieved 14 December 2021 form https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767).

[24] "For the certification or labelling of trusted data intermediaries, a lower intensity regulatory intervention was envisaged to consist in a softer, voluntary labelling mechanism, where a fitness check of the compliance with the requirements for acquiring the label as well as awarding the label would be carried out by competent authorities designated by Member States (which can also be the one-stop shop mechanisms also established for the enhanced re-use of public sector data)." [Ibid. p. 5].

[25] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (Text with EEA relevance) PE/81/2018/REV/1.

Digital Rights Management (DRM), Rights Expression Languages (REL), Open Digital Rights Language (ODRL), Licensed Linked Data Resources (LLDR) and Creative Commons Licenses have been worked out for twenty years now[26]. The last developments are proposing ODRL for compliance checking against GDPR and business policies (modelling both in a policy pipeline) [129], using refined vocabularies recently proposed by W3C's *Data Privacy Vocabularies and Controls Community Group,* (DPVCG) [130]. Another example is furnished by eFLINT, a domain-specific language developed for formalising norms based on transition systems and in Hohfeld's framework of legal fundamental conceptions [131].

3.5. Socio-Legal Governance for Hybrid Intelligence

There have been many proposals to coordinate norms and rights in artificial environments using AI or algorithmic governance. Akata et al. [132] recently launched a research agenda for hybrid intelligence, augmenting human intellect with collaborative, adaptive, responsible, and explainable AI. They define hybrid intelligence (HI) as "the combination of human and machine intelligence, augmenting human intellect and capabilities instead of replacing them and achieving goals that were unreachable by either humans or machines" [132] (p. 19) and formalize four challenges: (i) *Collaborative* HI: How do we develop AI systems that work in synergy with humans? (ii) *Adaptive* HI: How can these systems learn from and adapt to humans and their environment? (iii) *Responsible* HI: How do we ensure that they behave ethically and responsibly? (iv) *Explainable* HI: How can AI systems and humans share and explain their awareness, goals, and strategies? The most interesting contributions, for purposes of this article, are the research questions related to these challenges. Some of them, pointing at validation and ethics, are specially interesting for us. We will return in … to the evaluation process, focusing in this discussion on the causal chain that can be built to assess legal validity:

> *What are the appropriate models for negotiation, agreements, planning, and delegation in hybrid teams? What is the best way to verify the agent's architecture and behaviour to prove their ethical "scope" (ethics in design)? What is the best way to measure ethical, legal, and societal (ELS) performance and compare designed versus learning systems (ethics in design)? Which methodology can ensure ELS alignment during the design, development, and use of ELS-aware HI systems (ethics by design)? How can explanations be personalized so that they align with the users' needs and capabilities? How can the quality and strength of the explanations be evaluated?*

Autonomy and self-organization are key concepts to understand the human/machine interface in socio-technical systems (intertwined systems consisting of human agents, technological artifacts, and institutional rules). Pitt et al. [133] proposed the idea of algorithmic *reflexive governance* for socio-techno-ecological systems through algorithms for deliberation, introspection, and self-organization. They focus on reflexivity as "the ability of a structure, process, or organization to reconfigure itself in response to reflection upon its own performance". In a slightly different line of thought, stemming from Deming's idea of evolutive rational management and Alexander's ideas on habitability [134], position the concept of *conscious design* (CD) for this new space in which platform-provided affordances (e.g., "buy", "like", and "ban") and online participants' expectations are putting new constraints. Online institutions (OI)—or 'electronic institutions'—play a significant role, as they are able to regulate the interaction of human and artificial agents online, or in multi-agent systems (MAS) within a Value Sensitive Design (VSD).

> *OIs contain policies that facilitate the governance of participant activity, either through what a participant is allowed to do in certain circumstances or what a participant may choose (not) to do for the sake of any social consequences. Online institutions*

[26] See the work by the Open Digital Rights Language Community Group led by Renato Iannella at W3C, (Retrieved 16 December 2021 from https://www.w3.org/community/odrl/).

> *embody both affordances and norms. [. . .] the sociotechnical systems complement of object-oriented programming's Model-View-Controller (MVC), where the world (W) is a collection of social spaces, that are sub-contexts of the real world, institutions (I) are the policy frameworks into which the values that characterise the system are imbued, and the technological space (T) where online inter-actions are processed according to software representations of the institutional conventions.* [134] (pp. 2–4)

This is the WIT (World + Institution + Technology) metamodel, i.e., a framework for the operationalization of the CD values in the construction of socio-technical systems. Resuming this metamodel Noriega and Casanovas [135] recently defined five levels of autonomy in the governance of autonomous systems. At the first level there is an instrumental delegation in which, once a process has been defined, the AI system automatically makes the decisions that are applied to a task—or a well-defined part of the process—within a predefined universe of situations. Some examples are ROOMBA, automatic text translators or automatic imaging assistants, in which their expertise is limited to a well-defined task. Increasing degrees of complexity follow. Teleological, competent-responsible agents combining reasoning capabilities and ontologies (e.g., crowdsourcing processing, CyC, and DBpedia), and agents endowed with some moral competence in the social world (patient assistant robots, GMT-3, 4-5 level Coordinated Autonomous Vehicles) would integrate the next levels of autonomy. The fifth level is still to come, integrating general human intelligence into artificial systems. This will take time. However, handling and controlling evolving hybrid intelligence is the next step in the so-called *Internet of Autonomous Things* (IoAT). Scalability is also a key issue in IoAT [136].

Likewise, Theodorou and Dignum [137] call for an "actionable policy to assess, develop, incentivise and support the use and development of AI" that "should thus focus on social aspects of AI". They convincingly call for a more granular down-to-earth specification of *ethical and socio-legal governance*. Mechanisms of legal compliance should figure out concrete ways to implement, apply and enforce in a more specific way ethical general principles and policies. Ethics for AI development play a central role in this formulation, but research should be able to find some concrete paths to further develop general principles. We will follow this thread later, as our proposal to understand the four clusters of the metarule of law scheme according to a driver or enabler system approach is related to this claim for a better and more granular specification.

3.6. Legal Compliance: Compliance through Design

From a practical perspective, legal compliance or Compliance *through* Design (CtD) holds several features that are related to the conditions fostering legal ecosystems. Among them: (i) it is *intermediate*, i.e., at the crossroads of LOD, IoT and Industry 4.0 (i.e., it should be carried out on real time scenarios, using linked, interoperable data); (ii) *semi-automated* (not full or hardcoded, as human intervention is always needed at several stages, i.e., first to interpret legal and ethical provisions, and then to control and monitor the results); (iii) *hybrid* (as semi-automation entails the activation of hybrid intelligence, between humans and machines); (iv) *modular* (as it requires the construction of models using norms, principles and values stemming from different sources: hard and soft law, policies, and ethics); (v) *adaptive* and *scalable* (dynamic not static, to accommodate legal changes); (vi) *partial* (as full compliance is not always possible: This means the establishment of accepted thresholds) [88]; (vii) *adjustable* to the different typologies of PaaS (Platform as a Service) economies (i.e., platform-driven solutions can be centralized or decentralized, private or shared, normal or cryptocurrency oriented, etc.) [138]; and (viii) *flexible* to overcome the difference between 'internal' corporate/organizational policies and 'external' legally-driven processes from a middle-out/inside out approach (i.e., encompassing regulatory systems considering properly the legal perspective as a third dimension, linked to the social scenarios and formal languages of Industry 4.0).

This raises the interesting question of the nature of legal requirements. In computer science and engineering, functional requirements specify what the software system must do,

non-functional requirements specify, among others, how well the system shall perform its functions [139]. In legal computer science and engineering, the definition and identification of legal requirements have drawn much attention, with different methodological trends regarding the specific systems and tools at stake but combining goal-oriented requirements engineering tools, defeasible logic, NLP, and ontology building [140–143]. In https://lynx-project.eu/ (LYNX) (accessed on 27 December 2021), we differentiated between *functional requirements* (referring to what is expected from legal web services) and *systemic requirements* (referring to broader system expectations related to law firms) [144][27]. But LYNX is a SMEs' legal compliance service. In other Industry 4.0-oriented platforms focused on *smart* and *intelligent* manufacturing such as OPTIMAI[28], an integration of both systemic and functional requirements would be better suited for legal governance validation purposes. Think of real time scenarios with augmented reality (context-aware environment using AR glasses to optimize production chains) and digital twins (digital technology allowing the virtualization of the production process) [145].

3.7. Beyond the AI4People SMART Model for Legal Governance

From a legal point of view, much work has already been done on legal compliance and validation processes. Boella (Boella et al. [146]), Ghavanati (Boella et al. [146]), Palmirani (Monica Palmirani [147]), Governatori [83], Bartolini [148] Robaldo [148], among many other researchers of the AI and Law community, have richly seeded the regulatory field mainly from a computational stance, working on legal ontologies, semantic languages, rules, and defeasible logic modelling. Legal theory and legal reasoning have also been fleshed out from an AI and analytical philosophy approach for more than three decades now [149]. We are focused on a more detailed description of the sociolegal field, especially on the variety of behaviours, conceptual mindsets and tools that are transforming it in a complex processing information network at different levels.

Both for the private and public sectors, the SMART model of AI governance—scalable, modular, adaptable, reflexive, technologically-savvy—that was presented by AI4People to the EU Parliament in November 2019 recommended 14 PriorityActions that can be undertaken within three new groups of priority: (i) forms of engagement[29]; (ii) top-down no-regrets actions[30]; and (iii) middle-out coordination mechanisms for the governance of AI[31]. Note that these three approaches portrait the law from the implementation point

[27] We identified functional and systemic requirements. The first ones were users' requirements and led to building functionalities on the https://lynx-project.eu/ (accessed on 27 December 2021) (LYNX) platform. For instance, (i) monitoring law, jurisdictions, regulatory compliance and alert users in case of innovations and legal changes, and (ii) providing access to tax law, labor law, required permits or necessary authorizations and operating licenses (etc.). Systemic requirements were more generic, denoting the properties of the legal 'ecosystem' the users intended to deal with. Law firms' representatives used several narratives to refer to what they expected from the system: "The notion of "*customization*" of the service, i.e., adaptation to the needs of different end-users, and the metaphor of "*radar*", as used in the legal focus group, suggest an intended meaning which is implicit in this kind of narratives: (1). Legal advisors provide a 'summary': arguments about key issues to make it easier for the lawyer to choose one strategy or another, taking into account the client's needs. (2). 'Our lawyers need to know that they know everything. We are like a radar system. In this regard, we should have a lead on the way the market is developing from a technical or legal perspective'." [144] (p. 32).

[28] OPTIMAI (https://optimai.eu/ accessed on 27 December 2021): Optimazing Manufacturing Processes through Artificial Intelligence and Virtualization.

[29] I.e., as defined in the Report [12]: "cross-disciplinary and cross-sectorial cooperation—and debate—on the issues of AI, the creation of an European observatory for AI, and of legally deregulated special zones, or living labs, for AI empirical testing—and development for a better interaction between scientists and laymen. By taking into account today's limited understanding of the stakes of AI, the creation of new type of forums for collective consultation and discussion becomes a priority".

[30] I.e., as defined in the Report [12]: "the achievement of sustainable development goals, such as capacity building in a good AI society; an interoperable AI strategy between the EU and Member States; a support for the capacity of corporate boards of directors to take responsibility for the ethical implications of companies' AI technologies; strategies of inclusive innovation; the creation of educational curricula around the impact of AI and a coherent European AI research environment".

[31] i.e., as defined in the Report [12]: "represent a sort of interface between top-down and bottom-up approaches, that is, between the different forms of engagement and the set of no-regrets actions. These coordination mechanisms include participatory procedures for the alignment of societal values and understanding of public

of view as 'legal regulation', thus, trying to describe how mechanisms of governance are contained and handled into legal practices and legal documents such as the GDPR. For instance, forms of co-regulation are defined by Recital 44 of the 2010 AVMS Directive and Article 5(2) of the GDPR. The 2019–2020 pandemic has fuelled the mechanisms of governance inserted into legal documents and provisions.

In this sense, the notion of 'legal governance' is used, i.e., assumed and displayed, without being specifically defined, although Pagallo et al. [12] go a bit further pointing out that legal governance specifies how to address the interaction between (i) law and ethics; (ii) general vs. sector-specific regulation; (iii) different needs that may be regulated; (iv) different levels of regulation (e.g., global, international, national, or regional); and (v) different ways of modernization of the legal framework. A legal governance toolkit of coordinating mechanism is presented, based on *middle-out* grounds, beyond hetero-regulatory (i.e., authoritative forms of law), co-regulatory, self-regulatory or monitored self-regulatory models of governance. It is proposed that an effective regulatory toolkit should include at least the elements of modular adaptability, systemic interdependence, semantic interoperability, organic decentralization, intermediate conceptualization (logical intervenients), and abductive (inferential) reasoning for AI systems. Not all of them can be present at the same time or can be implemented with the same level of maturity.

Inferring abstractions from current sensor observations, converting raw data into machine-interpretable abstractions [150,151], aligning NLP and rule modeling, and annotation methodology in semantic languages is a matter of research. Modeling abductive (semiotic, associated, situated) and streaming reasoning in a usable way is still a difficult problem [152–154]. Likewise, aligning systemic interdependence, semantic interoperability and organic decentralization constitutes a challenge. But confronting these conditions and finding some solutions is essential to facilitate the emergence of socio-legal ecosystems, including ontologies, blockchain technologies and smart contracts[32]; and the regulation of processes and supply chains of Industry 4.0 (system control, quality control, fault diagnosis, predictive maintenance) [155].

We reproduced in Figure 2 the wind rose SMART model, with slight changes, as self- and co-regulation can adopt nuanced forms (including benchmarks and sandboxes) [7] and can be monitored and linked to standards, protocols, policies, and ethical bodies. We have already shown that this is feasible using hard-law instruments (such as legislative and case-based law) as well. Thus, the idea is that a middle-out approach can show these nuanced forms of self- and co-regulation, and it is not necessary to get stuck to the initial clustering proposed in Figure 1 as sources of law.

This scheme should be understood as a set of initial *drivers* that can be used to create many *enabling systems* to enhance citizens' rights. Note that, especially in the convergence of LOD, IoT, and Industry 4.0, rules operate at least at three different layers of perception, network, and application. So do the instruments and simulations of quality control, augmented reality, and digital twins in Industry 4.0, as explained above. From the legal side, this means that data flows in real time must comply with the protections of the metarule of law in a situation of multi-stakeholder governance [8], with the plural participation of all subjects involved along the production and distribution chain. This kind of requirements and conditions for legal and ethical compliance cannot be checked externally. Legal compliance checking must be initiated from the inside, and then reach other external control and monitoring layers (the last resort being the case-based law system). The taken perspective matters, as the implementation of the rule of law through enforcement is crossed in all clusters by social dialogue and its (online and offline) *relational* side. Figure 3 depicts

opinion, upstream multi-stakeholder mechanisms for risk mitigation, systems for user-driven benchmarking of marketed AI offerings, cross-disciplinary and cross-sectorial cooperation, and a European observatory for AI to consolidate these forms of coordination.

[32] As proposed by ONTOCHAIN, a New Generation Internet hub for start-up companies. Cf. https://ontochain.ngi.eu/ (accessed on 27 December 2021).

the orthogonal projection of this *inside-out approach* that complements and extends the middle-out one.

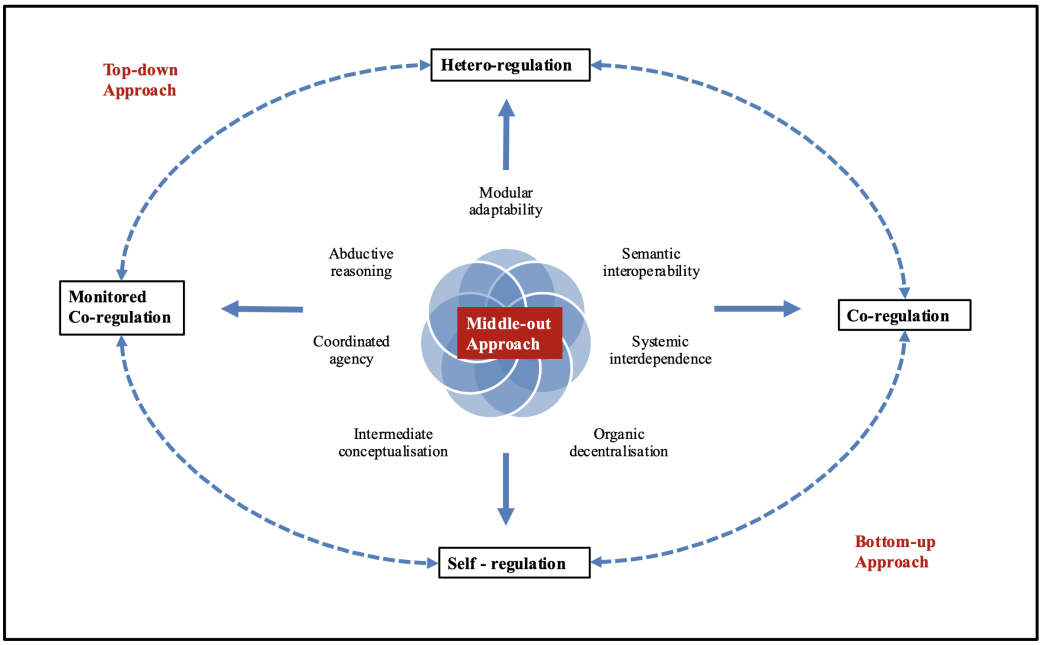

Figure 2. AI4People: SMART Good Governance Model (adopted from Pagallo et al. [12,156]).

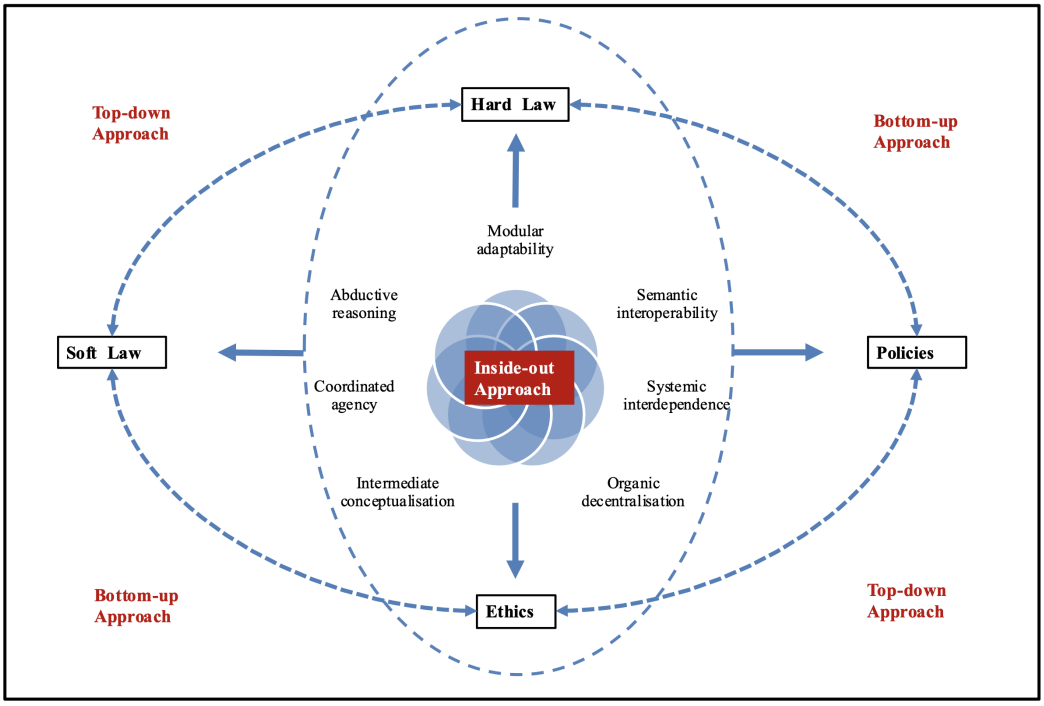

Figure 3. Inside-out Approach to LoD, WoD, and IoT regulatory systems.

3.8. Driving and Enabling Systems

As new technologies evolve, socio-legal governance models must change to meet human and social needs. As said, the legal instruments clustered in the scheme depicted in Figure 1 can also be understood as *drivers*, *driving systems* enabling communication between norms and their implementation. But when we refer to agents (stakeholders, rulers, regulated…) we need another category to describe their relationships with the regulatory system, distinct from capability or power, i.e., outside of the well-trodden path

of Hohfeldian jural concepts or the deontic description of 'power'. *Empowerment* is a different category than holding a 'subjective right' (Civil Law) or a 'power' (Common Law). It refers and enriches the affordances of the human and/or the artificial system at the perception level as well. Our intuition is that its validation process, i.e., the causal chain that can be built to check its degree of compliance with legal regulatory models, cannot be completely captured either by the Searle's formula `X counts as Y in context Z` nor from institutions defined as a set of constitutive rules (or counts-as conditionals logic). Making sense of law entails a different modeling process than assessing meaning. Determining the way to check legal validity is an empirical process. Validating—'making sense'—requires a complex selection and combination of the right variables at different level of depth to be explanatory and to properly ground a reusable toolkit.

This is not the place to explore it more comprehensively, but this attribute and its values (empowerment and being empowered) can be better described in a representation (democratic) context as political form. Its 'validity' or 'legality' does not come from the fulfillment of a norm (or from a rule extracted from the norm) but from a whole set of facts related to the empowerment framework. This is the reason why logic, semantic rules, business languages, and compliance regulatory models [6] have a role in it as valuable tools, they are necessary conditions but not sufficient, as they cannot build and proof by their own the empirical validation chain.

Following Pitkin's intuition about political representation [106,157], we would say that 'empowering' a cognitive agent means *'made its self-representation present'*, acquiring and exercising *a political power of self-representation,* i.e., a 'legal' power that is phenomenologically different from the representation of power as a deontic capability. This points out to the dimension of rights as *enablers* and to *digital sovereignty* as a possible basis for the socio-legal ecosystems created by enabling systems. But, as said, we cannot explore this line of thought here and it can only be drafted without the discussion that it certainly deserves, although *CivicTech* systems—platforms and applications for political participation; corruption, online hate, and fake news monitoring; crisis disaster-management; community building; assistive technologies…—would benefit from this analysis. We do not solely understand CivicTech as systems to enhance the relationship between the people and government, but to *enable* their users as self-driven, self-empowered citizens [158].

Another example of such socio-legal ecosystems is provided by the evolution of Online Dispute Resolution (ODR), in which access to justice has also been expanded with little or no government intervention. This is an example of *enabling systems* mainly situated at the axis of dialogue and relational law at the societal level. Born in the last third of the past century in commercial and business environments and within the civil society, ODR systems have been boosted in the 21st century with the evolution of agreement [159], negotiation, mediation, and conflict resolution technologies [60]. In a similar way to AI governance, ethics play a central and increasingly regulatory role in their evolution, but it has yet to be developed and enhanced [160].

Colin Rule, the former director of ODR for eBay and PayPal between 2003 and 2011, has recently written on the future of justice. He also underscores the need of a hybrid, entrenched Machine-Human cooperation on automating and improving justice systems to avoid unduly and biased systems.

> *Technology is now starting to disrupt the law. These changes are not being driven primarily by lawyers, bar associations, judges, or court administrators. They are being pushed most significantly by the disputants and litigants themselves. Because citizens utilize technology in almost every area of their lives, they now expect that when they encounter a dispute or file a lawsuit they will have access to similar kinds of tools to help them manage that process.* [59]

Covid-19 fueled this approach, fostered by new ways of understanding what is a dispute resolution mechanism. Entrepreneurs are using blockchain technology to create new ones, and existing mechanisms of dispute resolution that might feed into blockchain-

based smart contracts can be arrayed alongside new blockchain-based dispute resolution mechanisms [161].

4. Conclusions

We provided in this article a general overview of how the convergence of the WoD, the IoT, and Industry 4.0 challenge society to provide appropriate legal governance responses. It is our contention that the convergence of these technologies (in plural) is challenging the way law was understood, drafted, and applied in the 20th century. However, new is old, *gaudium cum pace*. This does not mean that all legal instruments and practices are all changing at the same time and at the same rate. The way how new behaviours and institutions emerge, how self-organized groups relate and create new collective properties, how legal practitioners and computer scientists are creating a big flourishing legal web services market, and how technology is pervading all dimensions of our lives (including work, manufactures, production and distribution chains) reaches our cognitive stages of perception, memory, and reasoning. It is a civilization change. However, legal concepts and architectures have a long history which sometimes pushes us back (and forth) again. Smart contracts, first, are contracts, and the existence of political forms and powers are not a big novelty either. Likewise, agreements, negotiations, mediations, and tools for conflict resolution can be infused into toolkits that were not born today. This holds for private and public law, either in Civil and Common law cultures, even if a digital public space and the transnational rule of law have yet to be created. Therefore, what is the message?

The current legal principles will continue to apply in many non-Industry 4.0 and IoT environments. There and in that context the current understanding of Law will still remain valid. However, more will be required to assure their appropriate application to the convergence of the WoD, the IoT, and Industry 4.0. We will therefore have parallel systems of legal governance until the global reality is fully immersed in technology. We cannot predict how technological and non-technological environments and scenarios will intertwine and for how long. Our intuition is, however, that the transitional period will produce new regulatory trends and many new questions.

If we return to the research questions about *socio-legal governance for hybrid intelligence*, we can observe that, after identifying the problems to be solved, some methodological and substantive regulatory issues remain. Especially the need (i) to redefine the elements, entities, properties and relationships that integrate the legal regulatory field in the new scenarios of the WoD, IoT, and Industry 4.0; (ii) to find a suitable methodology and theory to foster and then validate the legal ecosystems that will cross the dimensions (societal, legal, technological) and layers (sensory, network, application) of the IoT; (iii) to find the suitable theories and metrics to build a testable and reliable legal governance mindset. There are big challenges as well in the expressivity of languages, i.e., about the extraction, conversion and representation of concepts and norms as they appear in natural languages into algorithms and formal languages with a high degree of expressivity. This has not been completely solved.

In this article we explored aspects of the notion of legal governance that would be meaningful in the new digital environment. We progressed some of the work done on the metarule of law, and we have complemented the SMART middle-out with an inside-out approach to digital regulatory systems. We made a few specific points, such as identifying (i) the need for an empirical approach to explain and validate legal information flows and the hybrid agents' behaviour, and (ii) the interest of a phenomenological and historical approach to legal and political forms, and (iii) the utility of separating enabling and driving regulatory systems. We did not describe in detail all the proposals about hard law, soft law, policies, and, especially, ethics, as that work requires a paper in its own right.

Author Contributions: Conceptualization, P.C.; Methodology, M.H.; Investigation, P.C., M.H. and L.d.K.; Original draft preparation, P.C.; Writing—review and editing, P.C., L.d.K. and M.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Casanovas, P.; González-Conejero, J.; de Koker, L. Legal Compliance by Design (LCbD) and through Design (LCtD): Preliminary Survey. TERECOM@Jurix 2017. In Proceedings of the 1st Workshop on Technologies for Regulatory Compliance, Luxembourg, 13 December 2017; Volume 2049, pp. 33–49.
2. Casanovas, P.; Rodríguez-Doncel, V.; González-Conejero, J. The role of pragmatics in the web of data. In *Pragmatics and Law*; Springer: Cham, Switzerland, 2017; pp. 293–330.
3. Casanovas, P.; Mendelson, D.; Poblet, M. A linked democracy approach for regulating public health data. *Health Technol.* **2017**, *7*, 519–537. [CrossRef]
4. Casanovas, P.; Koker, L.D.; Mendelson, D.; Watts, D. Regulation of Big Data: Perspectives on strategy, policy, law and privacy. *Health Technol.* **2017**, *7*, 335–349. [CrossRef]
5. Hashmi, M.; Governatori, G.; Lam, H.P.; Wynn, M.T. Are we done with business process compliance: state of the art and challenges ahead. *Knowl. Inf. Syst.* **2018**, *57*, 79–133. [CrossRef]
6. Hashmi, M.; Casanovas, P.; de Koker, L. Legal Compliance Through Design: Preliminary Results of a Literature Survey. In Proceedings of the 2nd Workshop on Technologies for Regulatory Compliance, Groningen, The Netherlands, 12 December 2018; Volume 2309, pp. 59–72.
7. de Koker, L.; Morris, N.; Jaffer, S. Regulating Financial Services in an Era of Technological Disruption. *Law Context.-Socio-Leg. J.* **2020**, *36*, 90–112. [CrossRef]
8. Poblet, M.; Casanovas, P.; Rodríguez-Doncel, V. *Linked Democracy: Foundations, Tools, and Applications*; Springer Nature: Cham, Switzerland, 2019; OA Law Brief 750.
9. Governatori, G.; Casanovas, P.; de Koker, L. On the Formal Representation of the Australian Spent Conviction Scheme. In *Rules and Reasoning*; Gutiérrez-Basulto, V., Kliegr, T., Soylu, A., Giese, M., Roman, D., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 177–185.
10. Rodríguez-Doncel, V.; Santos, C.; Casanovas, P.; Gomez-Perez, A. Legal aspects of linked data–The European framework. *Comput. Law Secur. Rev.* **2016**, *32*, 799–813. [CrossRef]
11. Rodríguez-Doncel, V.; Casanovas, P.; Araszkiewicz, M.; Palmirani, M.; Pagallo, U.; Sartor, V.A. *Explainable AI in Law, Law as Web of Data, Privacy, and the Rule of Law*; AICOL (2021). AI Approaches to the Complexity of Legal Systems. AICOL International Workshops 2018–2020: AICOL-XI@JURIX 2018, AICOL-XII@JURIX 2019, AICOL-XIII@JURIX 2020, XAILA@JURIX 2020. Revised Selected Papers on Explainable AI in Law, Law as Web of Data, Privacy, and the Rule of Law. LNAI, 13048; Springer: Cham, Switzerland, 2021.
12. Pagallo, U.; Aurucci, P.; Casanovas, P.; Chatila, R.; Chazerand, P.; Dignum, V.; Luetge, C.; Madelin, R.; Schafer, B.; Peggy, V. On Good AI Governance: 14 Priority Actions, a SMART Model of Governance, and a Regulatory Toolbox. In *AI4PEOLE*; Atomium Technical Report; Brussels, Belgium, 2019. Available online: https://ssrn.com/abstract=3486508 (accessed on 14 December 2021).
13. Aghaei, S.; Nematbakhsh, M.A.; Farsani, H.K. Evolution of the World Wide Web : From Web 1.0 to Web 4.0. *Int. J. Web Semant. Technol. (IJWesT)* **2012**, *3*, 1–10. [CrossRef]
14. Hendler, J.A.; Berners-Lee, T. From the Semantic Web to social machines: A research challenge for AI on the World Wide Web. *Artif. Intell.* **2010**, *174*, 156–161. [CrossRef]
15. White, B. Discovering the Future of the Web. *J. Comput. Inf. Technol.* **2015**, *23*, 87–93. [CrossRef]
16. Oztemel, E.; Gursev, S. Literature review of Industry 4.0 and related technologies. *J. Intell. Manuf.* **2020**, *31*, 127–182. [CrossRef]
17. Lu, Y. Industry 4.0: A survey on technologies, applications and open research issues. *J. Ind. Inf. Integr.* **2017**, *6*, 1–10. [CrossRef]
18. Drath, R.; Horch, A. Industrie 4.0: Hit or hype?[industry forum]. *IEEE Ind. Electron. Mag.* **2014**, *8*, 56–58. [CrossRef]
19. Almeida, F.L. Concept and dimensions of web 4.0. *Int. J. Comput. Technol.* **2017**, *16*, 7040–7046. [CrossRef]
20. Lee, J.; Bagheri, B.; Kao, H.A. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manuf. Lett.* **2015**, *3*, 18–23. [CrossRef]
21. Papcun, P.; Kajáti, E.; Koziorek, J. Human Machine Interface in Concept of Industry 4.0. In Proceedings of the 2018 World Symposium on Digital Intelligence for Systems and Machines (DISA), Košice, Slovakia, 23–25 August 2018; pp. 289–296.
22. Hermann, M.; Pentek, T.; Otto, B. Design principles for industrie 4.0 scenarios. In Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 5–8 January 2016; pp. 3928–3937.
23. Hofmann, E.; Rüsch, M. Industry 4.0 and the current status as well as future prospects on logistics. *Comput. Ind.* **2017**, *89*, 23–34. [CrossRef]
24. Lasi, H.; Fettke, P.; Kemper, H.G.; Feld, T.; Hoffmann, M. Industry 4.0. *Bus. Inf. Syst. Eng.* **2014**, *6*, 239–242. [CrossRef]

25. Umbarkar, A.; Serafin, N.; Betti, F. How fourth industrial revolution tech helped companies survive the COVID crisis. In Proceedings of the World Economic Forum, Geneva, Switzerland, 4 November 2021.
26. Howard, R.; Blanton, C.; Mendonsa, A.; Cannon, N.; Finnerty, B.; Lacheca, D.; Mickoleit, A.; Thielemann, K. *Technology Trends in Government, 2019–2020*; Gartner Report, Technical Report ID G00389782; Gartner: Gold Coast, Australia, 2019.
27. Mickoleit, A. *7 Ways to Maximize the Impact of Open Government Data: Lessons From France*; Gartner Report, Technical Report ID G00716846; Gartner: Paris, France, 13 April 2020.
28. Waddington, M. Research Note. Rules as Code. *Law Context* **2020**, *37*, 179–186.
29. Barraclough, T.; Fraser, H.; Barnes, C. Legislation as Code for New Zealand: Opportunities, Risks, and Recommendations. 2021. Available online: http://www.nzlii.org/nz/journals/NZLFRRp/2021/3.pdf (accessed on 14 December 2021)
30. Mendonsa, A. *Hype Cycle for Digital Government Technology, 2021*; Techreport—ID G00747518; Gartner: Paris, France, 2021.
31. Breuker, J. *Law, Ontologies and the Semantic Web: Channelling the Legal Information Flood*; IOS Press: Brentwood, TN, USA, 15 January 2009; Volume 188.
32. Athan, T.; Boley, H.; Governatori, G.; Palmirani, M.; Paschke, A.; Wyner, A. Oasis legalruleml. In Proceedings of the Fourteenth International Conference on Artificial Intelligence and Law (ICAIL '13), Rome, Italy, 10–14 June 2013; pp. 3–12.
33. Casanovas, P.; Rodríguez-Doncel, V.; Santos, C.; Gómez-Pérez, A. A European Framework for Regulating Data and Metadata Markets. In Proceedings of the 4th Workshop on Society, Privacy and the Semantic Web—Policy and Technology (PrivOn2016) Co-Located with 15th International Semantic Web Conference (ISWC), Kobe, Japan, 18 October 2016. Available online: http://ceur-ws.org/Vol-1750/paper-04.pdf (accessed on 21 November 2021).
34. Palmirani, M. Hybrid Model for Law in the Digital Era: A Dialogic Model through Text and Code. In Proceedings of the 3rd COHUBICOL Philosopher's Seminar on "Code-Driven Law", Organized Online, Brussels, Belgium, 9 November 2021.
35. d'Aquin, M.; Davies, J.; Motta, E. Smart Cities' Data: Challenges and Opportunities for Semantic Technologies. *IEEE Internet Comput.* **2015**, *19*, 66–70. [CrossRef]
36. d'Aquin, M.; Motta, E.; Sabou, M.; Angeletou, S.; Gridinoc, L.; Lopez, V.; Guidi, D. Toward a New Generation of Semantic Web Applications. *IEEE Intell. Syst.* **2008**, *23*, 20–28. [CrossRef]
37. Francesconi, E. On the future of legal publishing services in the Semantic Web. *Future Internet* **2018**, *10*, 48. [CrossRef]
38. Rehm, G.; Galanis, D.; Labropoulou, P.; Piperidis, S.; Welß, M.; Usbeck, R.; Köhler, J.; Deligiannis, M.; Gkirtzou, K.; Fischer, J.; et al. Towards an Interoperable Ecosystem of AI and LT Platforms: A Roadmap for the Implementation of Different Levels of Interoperability. In Proceedings of the 1st International Workshop on Language Technology Platforms (IWLTP'20) European Language Resources Association, Marseille, France, 11–16 May 2020.
39. Fensel, D.; Şimşek, U.; Angele, K.; Huaman, E.; Kärle, E.; Panasiuk, O.; Toma, I.; Umbrich, J.; Wahler, A. *Knowledge Graphs: Methodology, Tools and Selected Use Cases*; Springer Nature: Cham, Switzerland, 2020.
40. Kirrane, S.; Sabou, M.; Fernández, J.D.; Osborne, F.; Robin, C.; Buitelaar, P.; Motta, E.; Polleres, A. A Decade of Semantic Web Research through the Lenses of a Mixed Methods Approach. *Semant. Web* **2020**, *11*, 979–1005. [CrossRef]
41. The Law Society. Lawtech: A Comparative Analysis of Legal Technology in the UK and in Other Jurisdictions, London. 2019. Available online: https://www.lawsociety.org.uk/en/topics/research/lawtech-comparative-analysis-of-legal-technology (accessed on 16 December 2021).
42. Rakshit, U.; Koh, T.Y.; Xiaohan, C. *Legal Technology in Singapore*, 2nd ed.; LawTech. Asia: Singapore, 16 September 2019.
43. Mills, M.; Übergang, J. Artificial Intelligence in Law: An Overview. *Precedent (Sydney NSW)* **2017**, *139* , 35–38. Available online: https://search.informit.org/doi/10.3316/agispt.20172037 (accessed on 19 December 2021).
44. Blijd, R. DoA: Data on How Many Legal Tech Companies Rise & Die. 2019. Available online: https://tinyurl.com/bdcwsdnn/ (accessed on 14 December 2021).
45. Blijd, R. The Fall of Legal Tech and How to Pivot Out. 2020. Available online: https://tinyurl.com/4mpbke6u (accessed on 14 December 2021).
46. Blijd, R. Rebound: 10 Growth Areas in Our New Perimeter Prosperity. 2020. Available online: https://tinyurl.com/yckps7nj (accessed on 14 December 2021).
47. ILTA. *International Legal Technology Association Survey. Executive Summary*; International Legal Technology Association: Chicago, IL, USA, 2018.
48. ILTA. *International Legal Technology Association Survey. Executive Summary*; International Legal Technology Association: Chicago, IL, USA, 2019.
49. ILTA. Survey on Artificial Intelligence and Machine Learning. December 2019. Available online: http://epubs.iltanet.org/i/1193169-aiml19/0?_ga=2.81313303.1093332486.1578860678-709782971.1578860678 (accessed on 14 December 2021).
50. ILTA. *International Legal Technology Association Survey. Executive Summary*; International Legal Technology Association: Chicago, IL, USA, 2020.
51. ILTA. *International Legal Technology Association Survey. Executive Summary*; International Legal Technology Association: Chicago, IL, USA, 2021.
52. Soh, J.T.H. *The State of Legal Innovation in Asia-Pacific*; Research Collection School of Law, Singapore Management University: Singapore, 2019; pp. 1–176.
53. Blijd, R. How Big is the Addressable Market for the Legal Industry? 2021. Available online: https://tinyurl.com/2snj7f4v (accessed on 12 December 2021) .

54. INTAPP. *Form S-1 Registration Statement under the Securities Act of 1933*; Filed on Securities and Exchange Commission: Palo Alto, CA, USA, 2021.
55. Tung, K. AI, the internet of legal things, and lawyers. *J. Manag. Anal.* **2019**, *6*, 390–403. [CrossRef]
56. Schrage, M. AI is going to change the 80/20 rule. *Harv. Bus. Rev.* **2017**. Available online: https://hbr.org/2017/02/ai-is-going-to-change-the-8020-rule (accessed on 16 December 2021) .
57. Ashley, K.D. *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age*; Cambridge University Press: Cambridge, UK, 2017.
58. McCarty, L.T. *Research Handbook on the Law of Artificial Intelligence*; Chapter Finding the Right Balance in Artificial Intelligence and Law; Edward Elgar Publishing: Cheltenham, UK; Northhampton, MA, USA, 2018; pp. 55–87.
59. Rule, C. Online Dispute Resolution and the Future of Justice. *Annu. Rev. Law Soc. Sci.* **2020**, *16*, 277–292. [CrossRef]
60. Katsh, M.E.; Rabinovich, O. *Digital Justice: Technology and the Internet of Disputes*; Oxford University Press: Oxford, UK, 2017.
61. Gruber, T. Collective knowledge systems: Where the Social Web meets the Semantic Web. *J. Web Semant.* **2008**, *6*, 4–13. [CrossRef]
62. Mazhelis, O.; Luoma, E.; Warma, H. Defining an internet-of-things ecosystem. In *InInternet of Things, Smart Spaces, and Next Generation Networking*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 1–14.
63. Millard, C.; Hon, W.K.; Singh, J. Internet of Things Ecosystems: Unpacking Legal Relationships and Liabilities. In Proceedings of the 2017 IEEE International Conference on Cloud Engineering (IC2E'17), Vancouver, BC, Canada, 4–7 April 2017; pp. 286–291.
64. Moreno-Schneider, J.; Rehm, G.; Montiel-Ponsoda, E.; Rodriguez-Doncel, V.; Revenko, A.; Karampatakis, S.; Khvalchik, M.; Sageder, C.; Gracia, J.; Maganza, F. Orchestrating NLP Services for the Legal Domain. In Proceedings of the 12th Language Resources and Evaluation Conference (LRCE), Marseille, France, 11–16 May 2020.
65. Kerber, W. Data sharing in IoT ecosystems and competition law: the example of connected cars. *J. Compet. Law Econ.* **2019**, *15*, 381–426. [CrossRef]
66. Pagallo, U. *The Laws of Robots: Crimes, Contracts, and Torts*; Springer: Dordrecht, The Netherlands, 2013.
67. Bassi, E.; Bloise, N.; Dirutigliano, J.; Fici, G.P.; Pagallo, U.; Primatesta, S.; Quagliotti, F. The Design of GDPR-Abiding Drones Through Flight Operation Maps: A Win–Win Approach to Data Protection, Aerospace Engineering, and Risk Management. *Minds Mach.* **2019**, *29*, 579–601. [CrossRef]
68. Bassi, E. Urban Unmanned Aerial Systems Operations. *Law Context* **2019**, *36*, 1–12. [CrossRef]
69. Neves, F.T.; de Castro Neto, M.; Aparicio, M. The impacts of open data initiatives on smart cities: A framework for evaluation and monitoring. *Cities* **2020**, *106*, 102860. [CrossRef]
70. Smith, K.; Seligman, L.; Rosenthal, A.; Kurcz, C.; Greer, M.; Macheret, C.; Sexton, M.; Eckstein, A. "Big Metadata" The Need for Principled Metadata Management in Big Data Ecosystems. In Proceedings of the Workshop on Data analytics in the Cloud, Snowbird, UT, USA, 22–27 June 2014; pp. 1–14.
71. Curry, E.; Sheth, A. Next-generation smart environments: from system of systems to data ecosystems. *IEEE Intell. Syst.* **2018**, *33*, 69–76. [CrossRef]
72. Davies, T. Open Data: infrastructures and ecosystems. *Open Data Res.* **2011**, 1–6.
73. Reggi, L.; Dawes, S. Open Government Data Ecosystems: Linking Transparency for Innovation with Transparency for Participation and Accountability. In *Lecture Notes in Computer Science, Proceedings of the 5th International Conference on Electronic Government and the Information Systems Perspective (EGOV), Guimarães, Portugal, 5–8 September 2016*; Volume LNCS-9820, Electronic Government, Part 2: Open Government; Scholl, H.J., Glassey, O., Janssen, M., Klievink, B., Lindgren, I., Parycek, P., Tambouris, E., Wimmer, M.A., Janowski, T., Soares, D.S., Eds.; Springer International Publishing: Porto, Portugal, 2016; pp. 74–86.
74. Styrin, E.; Luna-Reyes, L.F.; Harrison, T.M. Open data ecosystems: an international comparison. *Transform. Gov. People Process. Policy* **2017**, *11*, 132–156. [CrossRef]
75. Najafabadi, M.M.; Luna-Reyes, L.F. Open Government Data Ecosystems: A Closed-Loop Perspective. In Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS-50), Waikoloa Village, HI, USA, 4–7 January 2017.
76. Zuiderwijk, A.; Janssen, M.; Davis, C. Innovation with Open Data: Essential Elements of Open Data Ecosystems. *Inform Polity* **2014**, *19*, 2. [CrossRef]
77. Leminen, S.; Rajahonka, M.; Westerlund, M.; Wendelin, R. The future of the Internet of Things: toward heterarchical ecosystems and service business models. *J. Bus. Ind. Mark.* **2018**, *33*, 749–767. [CrossRef]
78. Dasgupta, A.; Gill, A.; Hussain, F.K. A Conceptual Framework for Data Governance in IoT-enabled Digital IS Ecosystems. In Proceedings of the 8th International Conference on Data Science, Prague, Czec Republich, 26–28 July 2019; pp. 209–216.
79. Zdravković, M.; Zdravković, J.; Aubry, A.; Moalla, N.; Guedria, W.; Sarraipa, J. Domain framework for implementation of open IoT ecosystems. *Int. J. Prod. Res.* **2018**, *56*, 2552–2569. [CrossRef]
80. Singh, J.; Millard, C.; Reed, C.; Cobbe, J.; Crowcroft, J. Accountability in the IoT: Systems, Law, and Ways Forward. *Computer* **2018**, *51*, 54–65. [CrossRef]
81. Singh, J.; Pasquier, T.; Bacon, J.; Powles, J.; Diaconu, R.; Eyers, D. Big Ideas Paper: Policy-Driven Middleware for a Legally-Compliant Internet of Things. In Proceedings of the 17th International Middleware Conference (Middleware'16), Trento, Italy, 12–16 December 2016; ACM: New York, NY, USA, 2016.
82. Sadiq, S.; Governatori, G.; Namiri, K. Modeling Control Objectives for Business Process Compliance. In *Business Process Management*; Alonso, G., Dadam, P., Rosemann, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2007; pp. 149–164.

83. Governatori, G. The Regorous Approach to Process Compliance. In Proceedings of the 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop, Adelaide, Australia, 21–25 September 2015; pp. 33–40.
84. Hashmi, M.; Governatori, G.; Wynn, M.T. Normative requirements for regulatory compliance: An abstract formal framework. *Inf. Syst. Front.* **2016**, *18*, 429–455. [CrossRef]
85. Schwabe, D.; Laufer, C.; Casanovas, P. Knowledge Graphs: Trust, Privacy, and Transparency from a Legal Governance Approach. *Law Context* **2020**, *37*, 1–19. [CrossRef]
86. Weber, I.; Xu, X.; Riveret, R.; Governatori, G.; Ponomarev, A.; Mendling, J. Untrusted Business Process Monitoring and Execution Using Blockchain. In *Business Process Management*; La Rosa, M., Loos, P., Pastor, O., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 329–347.
87. Mendling, J.; Weber, I.; Aalst, W.V.D.; Brocke, J.V.; Cabanillas, C.; Daniel, F.; Debois, S.; Ciccio, C.D.; Dumas, M.; Dustdar, S.; et al. Blockchains for Business Process Management—Challenges and Opportunities. *ACM Trans. Manag. Inf. Syst.* **2018**, *9*, 1–16. [CrossRef]
88. Lam, H.P.; Hashmi, M.; Kumar, A. Towards a Formal Framework for Partial Compliance of Business Processes. In *AI Approaches to the Complexity of Legal Systems XI–XII*; Rodríguez-Doncel, V., Palmirani, M., Araszkiewicz, M., Casanovas, P., Pagallo, U., Sartor, G., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 90–105.
89. Trubek, D.M.; Santos, A. *The New Law and Economic Development: A Critical Appraisal*; Cambridge University Press: Cambridge, UK. 2006.
90. Trubek, D.M. Law and development: Forty years after 'Scholars in Self-Estrangement'. *Univ. Tor. Law J.* **2016**, *66*, 301–329. [CrossRef]
91. Pistor, K.; Xu, C. Governing emerging stock markets: Legal vs administrative governance.Corporate Governance: An International Review. *Corp. Governance Int. Rev.* **2005**, *13*, 5–10. [CrossRef]
92. La Porta, R.; Lopez-de Silanes, F.; Shleifer, A. The economic consequences of legal origins. *J. Econ. Lit.* **2008**, *46*, 285–332. [CrossRef]
93. Michaels, R. Comparative Law by Numbers? Legal Origins Thesis, Doing Business Reports, and the Silence of Traditional Comparative Law. *Am. J. Comp. Law* **2009**, *57*, 765–795. [CrossRef]
94. Hildebrandt, M. Algorithmic regulation and the rule of law. *Philos. Trans. R. Soc. Math. Phys. Eng. Sci.* **2018**, *376*, 20170355. [CrossRef]
95. Szabo, N. Formalizing and Securing Relationships on Public Networks. *First Monday* **1997**, *2*. [CrossRef]
96. De Filippi, P.; Mannan, M.; Reijers, W. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technol. Soc.* **2020**, *62*, 101284.
97. De Filippi, P. *Blockchain Technology as an Instrument for Global Governance*; Digital, Governance and Sovereignty Chair; Sciences Po's: Paris, France, 2021; pp. 1–16.
98. De Filippi, P. *Blockchain and the Law*; Harvard University Press: Cambridge, MA, USA, 2018.
99. Fink, M. *Blockchain and the General Data Protection Regulation*; Can distributed ledgers be squared with European data protection law? EPRS—European Parliamentary Research Service: Brussels, Belgium, 2019.
100. Governatori, G.; Idelberger, F.; Milosevic, Z.; Riveret, R.; Sartor, G.; Xu, X. On legal contracts, imperative and declarative smart contracts, and blockchain systems. *Artif. Intell. Law* **2018**, *26*, 377–409. [CrossRef]
101. Konashevych, O.; Poblet, M. Is blockchain hashing an effective method for electronic governance? *arXiv* **2018**, arXiv:1810.08783.
102. Konashevych, O.; Poblet, M. April. Blockchain anchoring of public registries: Options and challenges. In Proceedings of the 12th International Conference on Theory and Practice of Electronic Governance, Melbourne, VIC, Australia, 3–5 April 2019; pp. 317–323.
103. Heydebrand, W. Process Rationality as Legal Governance: A Comparative Perspective. *Int. Sociol.* **2003**, *18*, 325–349. [CrossRef]
104. Tamanaha, B.Z. *On the Rule of Law: History, Politics, Theory*; Cambridge University Press: Cambridge, MA, USA, 2004.
105. Simbirski, B. Cybernetic muse: Hannah Arendt on automation, 1951–1958. *J. Hist. Ideas* **2016**, *77*, 589–613. [CrossRef]
106. Pitkin, H. *The Concept of Representation*; University of California Press: Oakland, CA, USA, 1967.
107. Habermas, J. *Between Facts and Norms*; MIT Press: Cambridge, MA, USA, 1996.
108. Sassen, S. *Territory, Authority, Rights*; Princeton University Press: Princeton, NJ, USA, 2008.
109. Scheuerman, W.E. Economic Globalization and the Rule of Law 1. In *Constitutionalism and Democracy*; Routledge: London, UK, 2017; pp. 437–460. [CrossRef]
110. Tamanaha, B.Z. The Tension Between Legal Instrumentalism And The Rule of Law. *Syracuse J. Int. Law Commer.* **2005**, *33*, 131.
111. Omari, L.A.; Barnes, P.; Pitman, G. Optimising COBIT 5 for IT governance: examples from the public sector. In Proceedings of the ATISR 2012: 2nd International Conference on Applied and Theoretical Information Systems Research, Taipei, Taiwan, 27–29 December 2012; Academy of Taiwan Information Systems Research (ATISR): Taipei, Taiwan, 2012; pp. 1–13.
112. Gehrmann, M. Combining ITIL, COBIT andISO/IEC 27002 for structuringcomprehensive informationtechnology for management inorganizations. *Navus Rev. GestãO Tecnol.* **2012**, *2*, 66–77. [CrossRef]
113. Hardy, G. Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges. *Inf. Secur. Tech. Rep.* **2006**, *11*, 55–61. [CrossRef]
114. Mangalaraj, G.; Singh, A.; Taneja, A. IT Governance Frameworks and COBIT—A Literature Review. In Proceedings of the Twentieth Americas Conference on Information Systems (AMCIS), Savannah, GA, USA, 7–9 August 2014.

115. Shamsaei, A.; Amyot, D.; Pourshahid, A. A Systematic Review of Compliance Measurement Based on Goals and Indicators. In Proceedings of the Advanced Information Systems Engineering Workshops, London, UK, 20–24 June 2011; Salinesi, C., Pastor, O., Eds.; Springer: Berlin/Heidelberg, Germany; 2011; pp. 228–237.
116. Yeung, K. Regulation by blockchain: the emerging battle for supremacy between the code of law and code as law. *Mod. Law Rev.* **2019**, *82*, 207–239. [CrossRef]
117. Floridi, L.; Cowls, J. A Unified Framework of Five Principles for AI in Society. *Harv. Data Sci. Rev.* **2019**, *1*. Available online: https://hdsr.mitpress.mit.edu/pub/l0jsh9d1 (accessed on 14 December 2021). [CrossRef]
118. Braithwaite, J.; Drahos, P. *Global Business Regulation*; Cambridge University Press: Cambridge, MA, USA, 2000.
119. Black, J. Decentring regulation: Understanding the role of regulation and self-regulation in a 'post-regulatory' world. *Curr. Leg. Probl.* **2001**, *54*, 103–146. [CrossRef]
120. Nonet, P.; Selznick, P. *Law and Society in Transition: Toward Responsive Law*; Octagon Books: New York, NY, USA, 1978.
121. Drahos, P. *Regulatory Theory: Foundations and Applications*; ANU Press: Canberra, Australia, 2017.
122. Pohle, J.; Thiel, T. Digital sovereignty, Internet PolicyReview. *Alexander Von Humboldt Inst. Internet Soc. Berl.* **2020**, *9*, 1–19.
123. Floridi, L. The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philos. Technol.* **2020**, *33*, 369–378. [CrossRef]
124. Habermas, J. Postscript to Faktizität und Geltung. *Philos. Soc. Crit.* **1994**, *20*, 135–150. [CrossRef]
125. Ostrom, E. Crossing the great divide: Coproduction, synergy, and development. *World Dev.* **1996**, *24*, 1073–1087. [CrossRef]
126. Ostrom, E. Sustainable Social-Ecological Systems: An Impossiblity? In Proceedings of the 2007 Annual Meetings of the American Association for the Advancement of Science, "Science and Technology for Sustainable Well-Being", San Francisco, CA, USA, 15–19 February 2007.
127. Tuori, K. *Critical Legal Positivism*; Ashgate: Aldershot, UK, 2002.
128. Casanovas, P. Conceptulasation of Rights and Meta-Rule of Law for the Web of Data. *Rev. Democr. Gov. Electron.* **2015**, *1*, 18–41.
129. De Vos, M.; Kirrane, S.; Padget, J.; Satoh, K. ODRL Policy Modelling and Compliance Checking. In *Rules and Reasoning*; Fodor, P., Montali, M., Calvanese, D., Roman, D., Eds.; Springer International Publishing: Cham, Switzerland, 2019; pp. 36–51.
130. Bonatti, P.A.; Kirrane, S.; Petrova, I.M.; Sauro, L. Machine Understandable Policies and GDPR Compliance Checking. *KI-Künstliche Intell.* **2020**, *34*, 303–315. [CrossRef]
131. van Binsbergen, L.T.; Liu, L.C.; van Doesburg, R.; van Engers, T. *eFLINT: A Domain-Specific Language for Executable Norm Specifications*; Association for Computing Machinery: New York, NY, USA, 2020; GPCE 2020; pp. 124–136.
132. Akata, Z.; Balliet, D.; de Rijke, M.; Dignum, F.; Dignum, V.; Eiben, G.; Fokkens, A.; Grossi, D.; Hindriks, K.; Hoos, H.; et al. A Research Agenda for Hybrid Intelligence: Augmenting Human Intellect With Collaborative, Adaptive, Responsible, and Explainable Artificial Intelligence. *Computer* **2020**, *53*, 18–28. [CrossRef]
133. Pitt, J.; Dryzek, J.; Ober, J. Algorithmic reflexive governance for socio-techno-ecological systems. *IEEE Technol. Soc. Mag.* **2020**, *39*, 52–59. [CrossRef]
134. Noriega, P.; Verhagen, H.; Padget, J.; d'Inverno, M. Ethical Online AI Systems through Conscientious Design. *IEEE Internet Comput.* **2021**, *25*, 58–64. [CrossRef]
135. Noriega, P.; Casanovas, P. *Mirando Hacia El Futuro. Cambios SociohistóRicos Vinculados a la Virtualización*; Chapter "La Gobernanza de los Sistemas Artificiales Inteligentes" [The Governance of Artificial Intelligent Systems]; Centro de Investigaciones Sociológicas (CIS) [Ministerio de la Presidencia]: Madrid, Spain, 2022. (In Spanish)
136. Barbulescu, M.; Hagiu, A. Leveraging The Scalability: A Distributed Cloud for Tomorrow's Internet of Autonomous Things. *Sci.-Bull.-Econ. Sci.* **2020**, *19*, 30–37.
137. Theodorou, A.; Dignum, V. Towards ethical and socio-legal governance in AI. *Nat. Mach. Intell.* **2020**, *2*, 10–12. [CrossRef]
138. Derave, T.; Prince Sales, T.; Gailly, F.; Poels, G. Comparing Digital Platform Types in the Platform Economy. In *Advanced Information Systems Engineering*; La Rosa, M., Sadiq, S., Teniente, E., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 417–431.
139. Guizzardi, R.; Li, F.L.; Borgidac, A.; Guizzardia, G.; Horkoff, J.; Mylopoulos, J. *Frontiers in Artificial Intelligence and Applications*; Chapter An Ontological Interpretation of Non-Functional Requirements; IOS Press: Brentwood, TN, USA, 2014; Volume 14, pp. 344–357.
140. Ghanavati, S.; Amyot, D.; Rifaut, A. Legal Goal-Oriented Requirement Language (Legal GRL) for Modeling Regulations. In Proceedings of the 6th International Workshop on Modeling in Software Engineering, Hyderabad, India, 2–3 June 2014; Association for Computing Machinery: New York, NY, USA, 2014; MiSE 2014; pp. 1–6.
141. Bartolini, C.; Muthuri, R.; Santos, C. Using Ontologies to Model Data Protection Requirements in Workflows. In Proceedings of the JSAI International Symposium on Artificial Intelligence, Kanagawa, Japan, 16–18 November 2015; pp. 233–248.
142. Sartoli, S.; Ghanavati, S.; Siami Namin, A. Compliance Requirements Checking in Variable Environments. In Proceedings of the 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), Virtual Event, 13–17 July 2020; pp. 1093–1094.
143. Amantea, I.A.; Robaldo, L.; Sulis, E.; Governatori, G.B.G. Semi-automated checking for regulatory compliance in e-Health. In Proceedings of the 2021 IEEE 25th International Enterprise Distributed Object Computing Workshop (EDOCW), Gold Coast, Australia, 25–29 October 2021; pp. 318–325.

144. González-Conejero, J.; Teodoro, E.; Casanovas, P. Lynx D1.1 Functional Requirements Analysis Report. 2018. Available online: https://doi.org/10.5281/zenodo.1256836 (accessed on 27 December 2021).
145. Casanovas, P.; Hashmi, M.; de Koker, L. *A Three Steps Methodological Approach for Legal Governance Validation*; AICOL@JURIX 2021; Mykolas Romeris University: Vilnius, Lithuania, 2021.
146. Boella, G.; Tosatto, S.C.; Ghanavati, S.; Hulstijn, J.; Humphreys, L.; Muthuri, R.; Rifaut, A.; van der Torre, L. *Integrating Legal-Urn and Eunomos: Towards a Comprehensive Compliance Management Solution. In International Workshop on AI Approaches to the Complexity of Legal Systems*; Springer: Berlin/Heidelberg, Germany, 2013; pp. 130–144.
147. Palmirani, M.; Martoni, M. Legal Ontology for Modelling GDPR Concepts and Norms. In *Frontiers in Artificial Intelligence and Applications, Volume 313: Legal Knowledge and Information Systems*; IOS Press: Brentwood, TN, USA, 2018; pp. 91–100.
148. Bartolini, C.; Giurgiu, A. Towards Legal Compliance by Correlating Standards and Laws with a Semi-automated Methodology. In Proceedings of the Benelux Conference on Artificial Intelligence, Amsterdam, The Netherlands, 10–11 November 2016; Springer International Publishing: Cham, Switzerland, 2016; pp. 47–62.
149. Prakken, H.; Sartor, G. Law and logic: A review from an argumentation perspective. *Artif. Intell.* **2015**, *227*, 214–245. [CrossRef]
150. Endler, M.; Briot, J.P.; de Almeida, V.P.; dos Reis, R.; Silva e Silva, F. Stream-Based Reasoning for IoT Applications—Proposal of Architecture and Analysis of Challenges. *Int. J. Semant. Comput.* **2017**, *11*, 325–344. [CrossRef]
151. Reis, R.D.; Endler, M.; de Almeida, V.P.; Haeusler, E.H. A Soft Real-Time Stream Reasoning Service for the Internet of Things. In Proceedings of the 2019 IEEE 13th International Conference on Semantic Computing (ICSC), Newport Beach, CA, USA, 30 January–1 February 2019; pp. 166–169.
152. Ganz, F.; Puschmann, D.; Barnaghi, P.; Carrez, F. A practical evaluation of information processing and abstraction techniques for the internet of things. *IEEE Internet Things J.* **2015**, *2*, 340–354. [CrossRef]
153. Maarala, A.I.; Su, X.; Riekki, J. Semantic reasoning for context-aware Internet of Things applications. *IEEE Internet Things J.* **2016**, *4*, 461–473. [CrossRef]
154. Shreyas, J.; Jumnal, A.; Kumar, S.D.; Venugopal, K.R. Application of computational intelligence techniques for internet of things: an extensive survey. *Int. J. Comput. Intell. Stud.* **2020**, *9*, 234–288. [CrossRef]
155. Peres, R.S.; Jia, X.; Lee, J.; Sun, K.; Colombo, A.W.; Barata, J. Industrial Artificial Intelligence in Industry 4.0—Systematic Review, Challenges and Outlook. *IEEE Access* **2020**, *8*, 220121–220139. [CrossRef]
156. Pagallo, U.; Casanovas, P.; Madelin, R. The middle-out approach: assessing models of legal governance in data protection, artificial intelligence, and the Web of Data. *Theory Pract. Legis.* **2019**, *7*, 1–25. [CrossRef]
157. Pitkin, H. Representation and democracy: Uneasy alliance. *Scand. Political Stud.* **2004**, *27*, 335–342. [CrossRef]
158. Oboler, A.; Casanovas, P. The Web of Data's Role in Legal Ecosystems to Address Violent Extremism Fuelled by Hate Speech in Social Media. In *AI Approaches to the Complexity of Legal Systems XI–XII*; Rodríguez-Doncel, V., Palmirani, M., Araszkiewicz, M., Casanovas, P., Pagallo, U., Sartor, G., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 230–246.
159. Ossowski, S. (Ed.) *Agreement Technologies Vol 8. LGT Series*; Springer Science & Business Media: Cham, Switzerland, 2012.
160. Ebner, N.; Zeleznikow, J. No sheriff in town: governance for online dispute resolution. *Negot. J.* **2016**, *32*, 297–323. [CrossRef]
161. Allen, D.W.; Lane, A.M.; Poblet, M. The Governance of Blockchain Dispute Resolution. *Harv. Negot. Law Rev.* **2019**, *25*, 75–102. [CrossRef]