MIT Computational Law Report

The Potential and Limitations of Computational Law for Data Protection

Gianluigi Riva

Published on: Nov 24, 2020

License: Creative Commons Attribution 4.0 International License (CC-BY 4.0)

0.0 ABSTRACT

Computational Law is a growing interdisciplinary field that stands at the border of Law and Computer Science. Research in this field has shown benefits for businesses in automating the legal relationships and streamlining the legal interactions between parties. However, there currently exists a gap in the literature about the application of such approaches in the context of Privacy and Data Protection relationships. On the other hand, Privacy domains suffer from an expansion of theoretical legal conceptualization and protection, which is not followed in practice by an effective application. This study investigates how Computational Law systems can be applied and implemented in existing Privacy and Data Protection frameworks addressed in an EU-US comparative analysis, in order to fill the gaps between legal provisions and practical protection. Adopting a top-down approach in line with the classical Civil Law analysis, it addresses the potential applications, limitations and implementation of Computational Law systems applied to the realm of Privacy, with specific focus dedicated to the analytical legal interpretation of the GDPR. The study evaluates both the potentialities and limitations of Computational Law systems and their capability to interpret complex legal phenomena. The article concludes with the conceptualization of a new topic, Quantum Law, as a possible solution for the emergent complexity of automated interpretation Computational Law systems must address.

0.1 Keywords

Computational Law; Privacy; Data Protection; GDPR; Privacy by Design; blockchain; smart contracts; consent; Artificial Intelligence; Smart Speakers; HCI; Quantum Law; coding; Legal Logic.

1.0 Introduction

Privacy is a domain ripe for innovation. The proliferation of devices connected to the Internet and the ubiquity of data-producing applications in our daily lives have made one thing clear: the existing methods for dealing with Privacy and Data Protection are not equal to these modern challenges. The concept of Privacy Self-Management in the US,[1] the Right to be Forgotten in the EU,[2] and most notably, the European General Data Protection Regulation (GDPR)[3] have proven to be inadequate for the demands presented by technologies that people use daily. Examples of these failures are everywhere and include domains such as Social Media,[4] Credit Reporting,[5] allegedly discrete websites for adults to meet each other,[6] Government Offices,[7] and health data gathered from wearable devices.[8] Such concerns promise to be made worse by the looming rise of the Internet of Things (IoT) and Smart City technologies.

Existing privacy solutions are also brittle to further innovations. The GDPR is particularly notable here because of its practical incompatibility with the nature of blockchain,[9] as well as for the limitations it provides to automated data processing and related decisions.[10] The effect of these challenges has left many questioning what remains to be done.

As a concept of law, Privacy is customarily reactive. Our collective understanding of Privacy expands after new technologies are developed. Further, the tools used to enforce Data Protection regulations and protect the personal data of individuals are not suited to address such challenges. As an example, it stands to reason that not much ought to be expected from the police officer on a bicycle who tries to catch a criminal in an automobile. In the same way, little should be expected from a Privacy professional who does not use computational tools to address computational issues related to Privacy. Equally, little should be expected from programmers who are great at designing and implementing software but have little familiarity with the law.

Technology plays a dual and dichotomous role for privacy, as it enables the development of individual rights and related social wellbeing. On the other hand, technology is the first and most powerful threat that undermines privacy preservation. Law slowly tries to chase the horizon of technological threats to privacy, but with only a handful of practical outcomes and the result is that many challenging issues remain.[11]

Computational Law can represent an alternative approach to traditional regulatory frameworks by enhancing the abilities of governments to fill practical gaps with digital solutions that may be programmed to perform tasks that regulators simply cannot. Computational Law can stand in as a prophylactic counterbalance to technological threats, that may empower both legislators and individuals. Such an intervention could help restore privacy to a greater state than the one that currently exists.

As technologies continue to produce more data and richer data about our daily interactions, the vulnerabilities faced today will only continue to grow. As noted by privacy scholar Ryan Calo, Privacy shifts with technology and these shifts often occur rapidly.[12] As new technologies continue to be developed to use more intimate information about people, including genetic and biometric applications such as Human-Computer Interaction (HCI) and Brain Computer Interfaces (BCI), there will inevitably need to be more solutions developed.

Computational Law and Privacy share the common thread of being transversal fields somehow linked to technological advancements. Even if Privacy and Data Protection disciplines are relatively old concepts, the new legal regime provided by the European GDPR (2018) introduced some legal novelty for dealing with the emerging AI technologies. On the other hand, practical applications of computational law and its accessibility have only recently become more practical thanks to advances in

computer science. The features that connect the two fields conceptually may also serve as common ground to create a functional link between each other. This connection between the two fields is precisely why computational law will become increasingly important in the Privacy and Data Protection context, as new technologies continue to be developed.

As a framework for Privacy implementation, Computational Law can be preferable to existing approaches because it operates using many of the same methods and protocols as these new technologies and can provide a data subject's real-time control over the data processing. As an approach to solving for Privacy, a shift toward Computational Law would also represent a more measurable and adaptive path to regulating emergent computational technologies. However, this burgeoning approach requires a deep reflection on the current limitations that Computational Law systems (CLS) have in dealing with this legal domain. By its nature, law is an algorithm. It may be an algorithm that uses people, but it is an algorithm. And because algorithms can be interpretable as computer code, so can laws.[13] A CLS for privacy could make use of structured parameters that leverage code to dynamically enable privacy frameworks so that they might be better specified, evaluated, adapted, and audited to the challenges in this domain.[14] If properly adapted, a CLS for privacy rights could create novel ways to address many of the existing challenges associated with Privacy and Data Protection frameworks. Such an infrastructure also represents a more suitable tool for regulating emergent technologies such as HCI interfaces in IoT ecosystem, wearables, Speech Interfaces[15] and BCI.[16]

1.1 Outline

This study analyses the potential and current limitations of Computational Law systems applied to the domain of Privacy. The aim of the study is to i) assess how these strengths and weaknesses affect the capability of a CLS to interpret the codification of the GDPR and ii) evaluate which solutions can help overcome the limitations identified. The work of this paper pays special attention to the different conceptualizations of a CLS for privacy rights in both Common Law and Civil Law systems. Emphasis is given to the analysis of the single limiting aspects of CLS, in light of the formal structures required to create such systems. Indeed, CL systems must tackle a wide range of interpretative obstacles that range from programming, semantics and legal interpretation, to explainability, reproducibility, and bias. This hermeneutical analysis shows how these limitations may be overpassed through the application of an innovative, new theory to measure and understand legal phenomena, described hereafter as Quantum Law. Section 2.0 provides an overview of Privacy regulations in the US and the EU. Section 3.0 evaluates the extent to which Computational Law can serve as a partial solution to existing Privacy frameworks by exploring the extent to which existing laws and regulations can be expressed as code, looking at several examples of innovative schemes for approaching modern Privacy challenges. Section 4.0 provides an overview of the limitations of Computational Law systems,

specifically in the context of Privacy regulation. Finally, Section 5.0 proposes the notion of Quantum Law as a way to address increasingly sophisticated challenges of Privacy law through automated interpretation.

2.0 Overview of Privacy Regulation

Because of the amount of commerce that takes place in the United States and the European Union, the analysis of this paper focuses on these legal systems. As these legal systems are designed according to different conceptual approaches that can undermine their interoperability, analysis of each system is required.[17]

While it might take more work, analyzing each of these systems can also serve as an opportunity to improve global predictability and legal certainty by building a CLS that harmonizes a series of requirements for both systems of law.[18] For example, by cataloging the requirements for data protection under both EU and US law, and using declarative logic to formalize the obligations between parties from different countries using an expert system, as well as 'international smart contracts'[19] based on the choices of the parties (i.e., 'forum shopping'[20], *pactum de lege utenda*[21], and *'depeçage'* technique[22], according to International Private Law[23]) there is the opportunity to develop new incentives that can be helpful in reduce friction among businesses that rely on data for their business models and also empower consumers by specifying, more clearly a global set of rights.

The US and EU regulatory systems work according to different approaches, principles, and rules. Therefore, it is essential to highlight some of the key differences that can influence the codification of a CLS one direction or another. First, it must be considered that CL deals principally with the set of private relationships, primarily those that fall into the regime of private law, such as contract, tort, copyright, and so forth. And while these differences may seem irreconcilable, the underlying motivation of each is better aligned than it might appear both systems are aimed at a two-fold principle (i.e., the legal effects of a situation must be foreseeable because the Law must provide certainty).

Despite a shared foundation undergirding each respective notion of Privacy[24], the legal regimes of the United States and the European Union function in substantively different ways[25]. First of all, the EU has an organic regulatory framework for both Privacy and Data Protection, while the US relies only on a granular set of federal statutes that afford specific applications of the sole Privacy.[26] In Europe, both Privacy and Data Protection are fundamental rights. Even if the doctrine still has not defined a Theory of the Law regarding the matter, it can be said that Privacy concerns personhood rights, while Data Protection concerns procedural rights and duties, including security and system architecture. Indeed, it must be taken into account that the different legal system conceptualization influences the

respective Privacy paradigms and their effects. Indeed, the cultural backgrounds that inform the different legal regimes also have effects on the legal metaphors by which privacy is understood in the US and in Europe. This eventually affects the final legal effects that can be different in the two systems regarding the regime for the same legal situation. For instance, the significant differentiation between the two approaches relies on considering personal data as a property (in the US) and as immaterial goods with rights of disposition over them (in the EU).

2.1 European Approach to Privacy

Resultantly, the GDPR addresses each of these concepts by looking at protection to individuals (referred to as "data subjects"). In addition to the protection of personal data, the GDPR also grants protection to the data flow. This means that the GDPR protects conflicting goods and they must be balanced according to the case. However, there is in place a set of principles[27], which informs the regulation governing the data processing, which in turn must be grounded on typical[28] legal basis. Among them, consent has a preeminent factual position and must be paired by several characteristics, i.e. freely given, informed, specific and unequivocal. As privacy belongs to personality rights, it cannot be an object of property.

Contrasting with the privacy frameworks in the United States, in Europe there is no data ownership (in the sense of proprietary paradigm)[29] and personal data cannot be commercialized as material goods. On a practical level, this means that an individual in Europe owns the support in which the data are stored (i.e. a material good) and has rights of disposition over their stored personal data. In the same way, a data controller does not own any data subjects' personal data but has limited rights of disposition accorded by the GDPR, in order to perform data processing activities. The rights of a data controller under the GDPR overlap with its other set of subjective positions accorded by the realm of intellectual property rights (IP) and which include datasets, databases, statistical analysis and so on. Even so, under the GDPR, any information regarding an individual is still considered personal data. Therefore, if these intellectual property rights are held over information falling under this definition, they directly conflict with the data subject's privacy (personhood) rights and must be balanced consequently. It means that the data controller eventually will have limited disposition for its IP rights, as well.

In cases where these rights overlap, there is a conflict between two private interests: the data subject's personhood interest vs. the data controller's economic interest. Depending on the facts of the case, one may prevail over the other even when a valid consent has been given.[30] However, one pivotal element in the EU approach to such matters is that the consent alone is enough to render lawful the data processing but must be flanked with fairness, transparency, and limited purposes of the processing itself.[31] This joint composition of consent and principles reflects the conceptualization of individual

freedom from the Civil Law system, wherein: weaker parties must be protected against their own will, as in particular cases (e.g. minors[32], workers[33], consumers[34]) it may be influenced or to some extent coerced or, however, a stronger party may take unfair advantage of their weaker position. Therefore, in these cases, the consent is still granted as a form of individual agreement but is valid only when other legal requirements are matched.

2.2 United States Approach to Privacy

On the contrary, the United States approach to Privacy pursues the goal of regulating the processing of data in specific domains of economic activity, based on the specific risks to citizens concerning their status as consumers. Put in another way, Privacy is not an individual's fundamental right in the US but is instead a consumer right that is to be balanced against business needs. Therefore, the US legal framework perceives Privacy as an economic and consumer-centered concept. Indeed, the competent US authority to supervise the matter is the Federal Trade Commission (FTC), which is also tasked with monitoring the adherence of companies' behavior in accordance with their Privacy policies and other respective laws on privacy. Thus, in the US, privacy is understood according to the contractual paradigms. As mentioned, Privacy rights belong to the spectrum of publicity rights in the US. As such, these rights are subject to the property law paradigm of ownership and commercialization. Under this approach, the consumer's consent to data processing assumes a different conceptual meaning than the EU's, as it falls into the general legal regime of contract law, and, as such, the individual is not protected against its own agency. This follows the individualization of responsibility that comes with property paradigms and that contract law attributes to one's agency, meaning that an individual is not protected once consent has been yielded. In other words, under this conceptualization, the Law assumes the individual can negotiate their position or refrain from the agreement. If the individual is in a weak position, then it is their responsibility to bargain a better deal (and therefore, it is their 'fault' if they fail to do it).

As a practical matter, privacy protections in this domain are weakened by asymmetric leverage between those collecting data and the individuals producing it. This necessarily implies that a disparity exists between those who collect data and the individuals that help create the data. Unfortunately, this leaves individuals with weaker protections than they might otherwise have.

The US privacy paradigm also recognizes a lack of protection for information that is voluntarily given to third parties, under the "third-party doctrine," which states that people who freely provide information to third parties have "no reasonable expectation of privacy."[35] This means that information that is publicly available on sites like Facebook, Twitter, and YouTube cannot qualify as private information because it has voluntarily been given to third parties. However, the US statutes are more focused on data security rather than consumers' rights. Security is indeed perceived under Prosser's conceptualization of Torts[36] and the overall proprietary paradigm, which entails

appropriation as its opposite. US conceptualization of security seems to align with this latter, as a form of breach over one's property. In the US, Privacy and security are often perceived as two faces of the same coin, if not sometimes overlapping matters. This, however, is not the case in the EU, where security is a procedural aspect (requirement) of Data Protection.[37] In the US, the primary regulation for Privacy remains the federal Privacy Act of 1974,[38] then modified in 1980, which introduced general protection for citizens against the Government's investigation powers. However, the US still lacks a single federal law for regulating the collection and use of personal data as a whole discipline. Instead, it has a system of federal and state regulations that can sometimes overlap and, generally speaking, the right to privacy finds its core protection under the 4th Amendment of the Constitution.[39] Guidelines have also been developed by governmental agencies and industry groups, which do not have the force of law, but can be useful as a self-regulatory framework and considered best practices. [40]

Nevertheless, the United States currently lacks a federal regulation on Data Protection, per the EU's meaning of the term (i.e. as the field of procedural rights related to Privacy, such as, for instance, the right to be forgotten, the right to access, the right to portability and so on). The most GDPR aligned US regulation is the California Consumer Privacy Act of 2020 (CCPA), which is a state law and, therefore, does not apply at a federal level.[41] The CCPA introduces some regulatory aspects provided by the GDPR (even if it can be considered less strict than the GDPR), such as the right to disclosure (information), to access, to portability, objection and to erasure.

3.0 Computational Law to implement Privacy solutions

The promise of Computational Law represents an interesting opportunity to enhance Privacy solutions. Given the increasing presence of interactive technologies in everyday life, with the user-to-machine as well as the machine-to-machine interactions, human behavior and interactions are more and more amenable to being represented as data and metadata. Critically, many of these interactions involve relationships that have some legal effect and as new technologies proliferate, it will be incumbent upon society to develop more sophisticated ways to address these legal challenges. This structural determination of interactions as sets of data allows to represent them as code and, consequently, allows the codification of the law in computational terms to address these phenomena with programming code paradigms. The rest of this section explores the features inherent to this particular law-code connection and how they can help in designing a Computational Law system for privacy.

3.1 Technological phenomena represented as code

Computational Law will play a crucial role in the adoption of new and connected technologies. The IoT itself will challenge many of the existing interactions among B2C,[42] B2B,[43] and C2C.[44] The problem

does not stop there, however. As new business models are shaped around the connections enabled by these new machines, whole streams of commerce will necessarily evolve around the structures of various data protection regulations that may be applicable. The management of such complexity will require a reliable automated system to represent interactions as data, catalogue those interactions, identify trends and outcomes, and facilitate legally effective processes. This is precisely the role of a CLS.

Yet, the interconnected ecosystem of the future will not only be composed of sensors, but also by innovative technological solutions, such as Smart Speakers, Virtual and Augmented Reality as well as wearable devices. Among them, the so-called Wearable Brain-Computer Devices (WBCD)[45] will be a communicative tool, which already now enables direct communications between the human mind and machines. These technologies will further complicate the scenarios and the legal relationships among the involved parties. Additionally, the IoT revolution will be paired with the rise of Speech Interfaces as one of the primary tools for users to interact with the connected ecosystem. This may be the direction for implementing a virtual assistant to help computing the law and help users navigating the complexity of IoT interrelations and uncertain legal effects that will derive therefrom.

Given these scenarios, it can be argued that all these complex relationships will necessitate new types of regulations and could be managed directly by AI systems through coded programs. Indeed, every online relationship relies on programming and protocols, but only a few of them must conform to specific legal boundaries. The law usually adopts a neutral attitude toward technology: it requires only that the technology reach several minimum standards fixed as a basic threshold. Law also focuses on the effects rather than on the processes. Thus, the new body of technology entangled legal frameworks will lean on these two pillars. It derives that both the architecture of these systems and their functioning shall comply with these provisions, which in turn will have to deal with the complexity of the coded H2M and M2M interactions. It means that these tech-law codes shall be machine-readable in order to be implemented effectively.

3.2 Law represented as code

Computer Science, Language, Mathematics, and Law all share Logic as a methodological tool of analysis. Logic is the science of reasoning. Legal Logic focuses on the methodologies to understand the Law.[46] The Law is a coherent set of precepts expressed through language in a particular form. Therefore, the legal reasoning serves to build a coherent sequence of interdependent postulates in which one is the premise of the subsequent, and all concur to define the outcome, as the logical consequence of the analytical methodology. In order to understand the Civil Law legal interpretation approach (and to be able to encode them in a CLS), it is pivotal to comprehend the mechanisms of the Legal Logic, which differs from pure Logic under several aspects. For Legal Logic, the legal norm - i.e. the proposition - must be addressed first in the formal sense, namely for its structure independently

from its content. Logic instead addresses the content and its truth. Then, Legal Logic addresses the type of proposition according to its form (declarative, interrogative, imperative and exclamatory) and its function (descriptive or prescriptive).[47] Descriptive are those propositions that provide information, while prescriptive are those that provide instructions. Logic usually deals with the former, as descriptive propositions can be true or false, whereas prescriptive ones cannot be said as such. Prescriptions are instead evaluated as valid or invalid, just or unjust. It derives that the difference between Logic and Legal Logic is that the truth of a proposition can be demonstrated, while the justice of a norm can only be argued to persuade others (i.e. the Rhetoric).[48]

The Legal Logic Formalism doctrine[49] moves from the study of the proposition to develop the legal reasoning and Dialectic, Rhetorical, and formal interpretation as the methodologies to analyze a norm. Dialectic is the art of speech which relies on empirical methods. It tends to the persuasive argumentation by unifying the thesis and the antithesis in a synthesis. It exploits the syllogism as the principal tool of reasoning, which is expressed with a first general premise described by a logical quantifier (all, somebody, one, nobody) followed by a second particular premise that has a common term with the first one. Thanks to deductive reasoning, the interpreter finds a logical and coherent conclusion. The logical syllogism is considered categorical, as both the premises are apodictically true and so the conclusion is true as well. In the legal syllogism, however, the premises do not have to be true, and the conclusion is only plausible.[50]

Both the logical and legal syllogism have in common the "if-then" structure. What it is important to highlight here is that logical syllogisms rely on a binary outcome and so it is perfect for a machine-readable system because it belongs to Boolean logic. Instead, the legal syllogism escapes the true/false binary logic and deals with what Computer Scientists describe as "fuzzy-logic", in which the polyvalent logic can attribute to the proposition all the values comprehended between 0 and 1, i.e. the true/false classification. This suggests that Computational Law must deal with the second kind of logic in order to be fruitfully applied to legal reasoning.

Nevertheless, there is a further two-fold complication. The prescriptive proposition – i.e. the norm – is not true/false but valid/invalid, just/unjust, and applicable/non-applicable. Resultantly, a conclusion might be both 0 and 1 at the same time as well, as all the other 0-1 intervals contemporarily. In other words, the legal reasoning can result in a contradictory conclusion in which the outcome can be true and false at the same time; or it can be true, but not valid, and contemporarily just but not applicable, in a set of possible outcomes that comprehend all the combinations among the mentioned variables. This fact means that legal reasoning deals with logic more similar to that required by Quantum computing than fuzzy logic.

This conceptualization can be visualized according to the classical representation of the "QuBit" in comparison to classical "bits" (Figure 1). This aspect can be fundamental in the application of Computational Law outside of the mere compliance-checking.

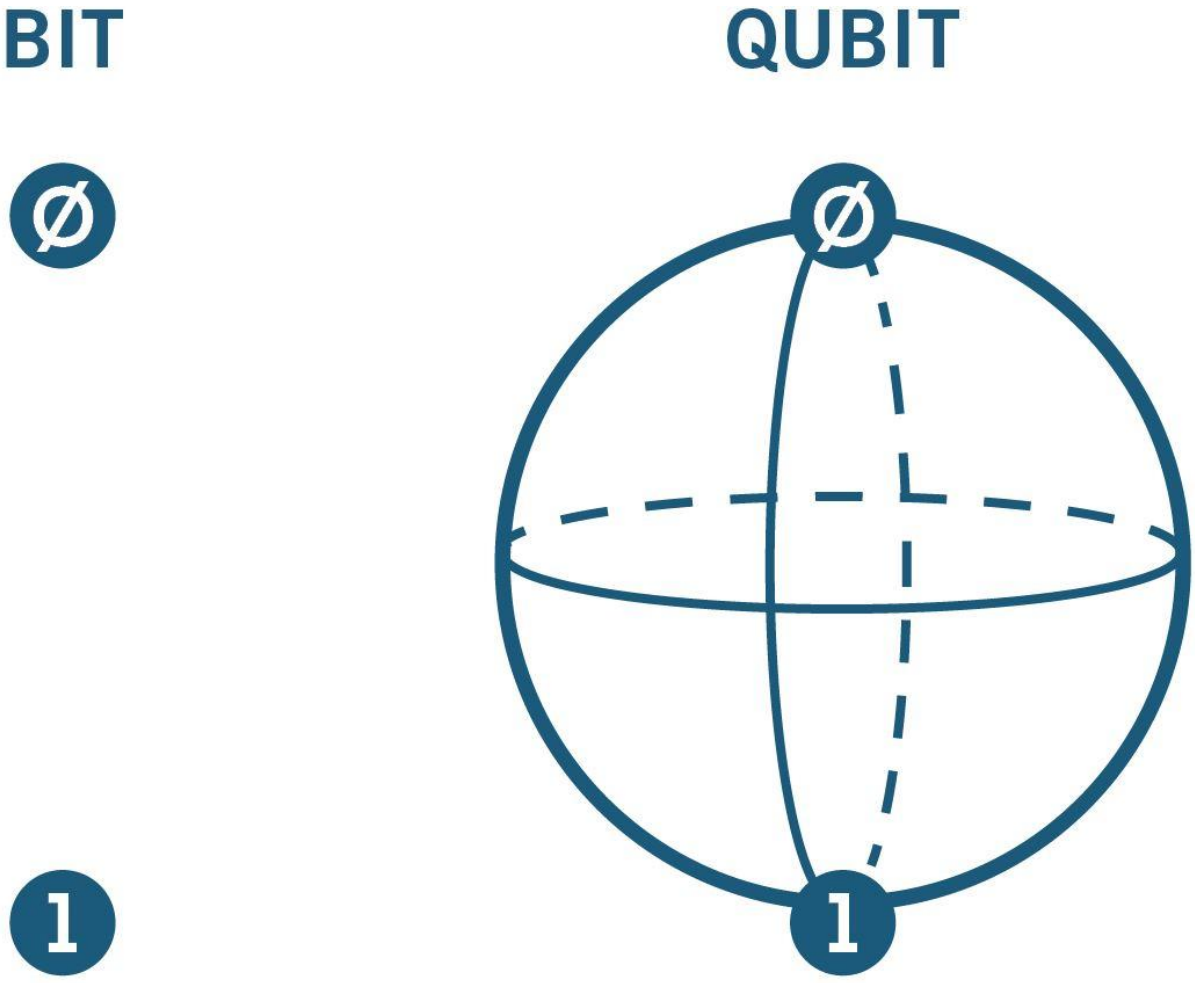


Figure 1[51]

The art of rhetoric deals precisely with this sophisticated space of possible combinations, as it is the art of structuring the right sequence of dialectic arguments to persuade others of the validity of an argument.[52] Rhetoric represents the most speculative form of legal reasoning, as it grounds on a set of techniques that, regardless of the logic, necessarily exploits the human linguistic abilities, such as tone, inflexion, volume, vocabulary, and sentence structure.[53] The principal rhetorical figures in the Theory of Argumentation[54] in legal reasoning are the analogy, the inverse reasoning, the "all the more reason" argument, and the reasoning for absurd.[55] Both Dialectic and Rhetoric tend to persuade because of the legal need for a juridical motivation (i.e., the explanatory principle), meaning that the outcome must be logically justifiable. As they both deal with the language and its structures and rules,

from a Computational Law perspective, these matters can cross with Computational Linguistics (i.e. the interdisciplinary field concerned with the statistical modelling of natural language in a machine-readable approach).[56] The promise of such developments is that these relationships can be used to better connect CL and Legal Logic with the realm of Speech Interfaces, namely a natural-language processing AI-based interface. Indeed, virtual assistants could be easily integrated with a CL self-help assistive interface in a 'Ross-like' feature, to help both professionals and individuals interpreting the law or used even to persuade another legal interpreter. In addition, the aim of Dialects and Rhetoric is to persuade, that is the capability of influencing others' behavior to modify it according to a predefined scope. This concept seems to overlap with the notion of Social Physics, as the social discipline that describes the mathematical connections among information and its repercussions on human-behaviors.[57] Social Physics aims to analyze the triggers that can model norms, productivity and collective behaviors thanks to social learning and ideas fluxes. Therefore, as Social Physics deals with mathematical models, its methodologies can start to be encoded into CL systems.

Privacy is a concept that can be defined in many contexts, from Law to Computer Science and from Philosophy to System Security. These matters represent the horizontal dimension of privacy. The vertical dimension of privacy addresses legal matters ranging from fundamental rights and Data Protection provisions down to security and programming procedure. However, this multidimensional characteristic of privacy requires interpreters to have experience in a diversity of backgrounds, and among which, there is no common language or taxonomy. In turn, this implies several issues when it comes to correctly interpreting the legal requirements and translating the legal provisions (preceptive propositions) into real answers for a legal regime to comply with. The privacy-applied legal syllogism (in fuzzy logic) should be simplified as much as possible to allow Computational Law being coded in a manner that ensures basic interpretation:

assumed true general preamble + assumed true specific preamble = plausible outcomes.

In order to illustrate how the legal reasoning works in a Privacy norm, we take the example of combined reading between two fundamental Data Protection provisions regarding the concept of lawful data processing. This illustrates what a Computational Law system should appropriately perform.

> **> GDPR art.6** "Lawfulness of processing":
>
> "1. Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; [...]"
>
> **> GDPR art.5** "Principles relating to processing of personal data"

> "1. Personal data shall be:
>
> a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); [...]"

The technical legal analysis of the norms must proceed with a formal literal reading. The keywords of Article 6(1) are "processing," "lawful," "only if," "at least," and, residually, "to the extent to". Data processing represents the object of the norm and refers to the definition given in Article 4(2).[58] This sets the ontological limitation of the precept: only what falls into the definition of processing can be lawful (so long as the required conditions occur). There is also another critical but silent reference to take into account: the norm applies only to that processing that falls into the provision of Article 2.[59] Other implicit references that inform the norm are the protected good, which is the personal data Article 1(1) and the limits provided by Article 1(3), which forbids the restriction of data flow within the European Union. The legal meaning of Article 6(1) is, therefore, the result of the syllogistic equation given by the terms above mentioned. Thus, "lawful" means protected by the law, and "only if" identifies the following options, which are only able to render the processing lawful if it is called an imperative list. The term "at least" is crucial and indicates that even just one of the listed options is sufficient to render the processing lawful.

Finally, the residual term "to the extent" individuates the internal limits of the lawfulness by cross-referring to the specific options listed. Namely, in the case of option a) (data subject's consent), the processing is lawful to the extent of the consent given. This subsumption opens another subset of cross-references, as it implies all the requirements for a valid consent ex GDPR Article 7 and the frame of the data processing declared by the data controller in the consent form.

The second level of the interpretation addresses Article 5(1), which defines the principles that apply to data processing. This kind of cross-referring among norms is called "combined reading" and helps to define, frame or understand the actual borders of a legal concept. Here, again, the analysis must refer to the literal meaning. In the simple precept given by Article 5(1), the object and protected good coincides with Article 6, i.e. the processing and personal data. The norm provides three characteristics that must apply to the processing and one limit. The three are lawfulness, fairness, and transparency, while the limit is the reference to the data subject. Now, the interpretation must rely on the syllogistic deduction: the three terms are listed separately, and both fairness and transparency do not define lawfulness. It derives that the processing is lawful when it matches the conditions provided by article 6 but do not necessitate to be fair and/or transparent to be lawful. Therefore, unfair and non-transparent processing is entirely lawful, and it remains valid, legitimate, and protected by the law even in the presence of a lack of fairness and transparency. Furthermore, the statement "in relation to

data subject" bonds the application of these principles toward the data subject only. Conceptually, it means that these three principles do not apply when the processing is managed toward third parties.

Finally, the combined reading of Articles 5 and 6 should also be informed by the connected recitals (39, 40, 42, 43, 44), which, however, are not binding and, in this case, do not provide any further element that may vary the analysis performed so far.

As seen, the miserable wording with which the addressed legal formulas are coded in the GDPR exposes the matter into a legal gray area. A higher degree of specification will be required of Computational Law Systems that purport to solve conflicts between the literal meaning of a norm and the accepted doctrine. Indeed, the level of complexity that a Computational Law System will be required to handle by new technologies means that new structures for managing Privacy will begin to emerge.

3.3 Computational Law Structures for Privacy

3.3.1 Privacy by Design

Privacy by Design is a conceptual approach to design interfaces and the related data processing.[60] It refers to the set of dynamic procedures and preventive technical solutions to grant transparent data processing to be compliant with privacy principles ensuring a user-centered focus. In the following decade, the concept gained popularity in the legal scholarship and was slowly recognized internationally in its final conceptualization. In 2012, the US Federal Trade Commission considered Privacy by Design in its report on Consumer Privacy as one of its three recommended practices for protecting online privacy.[61] It was then adopted in a positive regulation in 2016, and a similar concept was adopted GDPR but only came into effect in 2018.[62] In the GDPR, the concept of Privacy by Design, is referred to as 'Data Protection by Design.'[63] The regulation refers to the set of appropriate technical and organizational measures required, including: the implementation of data protection principles and the implementation of necessary safeguards for the processing of the data subjects' rights. Indeed, often in the United States, Privacy and Security are linked domains, if not overlapping ones. While in Europe, security is an aspect regulated under Data Protection. Thus, in the Computational Law context, it would be more accurate to refer to Data Protection by design, instead of Privacy by Design, since the former refers to the concept of technical measures and the latter should ontologically refers to a concept of rights. This concept refers to the necessity of providing the final user with data processing options (e.g., profiling, direct marketing, etc.) pre-set with opt-out selection by default. This means that the data controller is required to set the processing according to the data minimization principle, (i.e. to design the default data processing based on the solely necessary personal data that serves to provide the basic service).

This procedural nature of Privacy by Design and by Default can be addressed by Computational Law systems, which can be leveraged to help HCI programmers to design more trustworthy, transparent, and interactive structures for law and legal processes. CLSs can perform both an *ex-ante* and *ex-post* analysis of the interface structure to check that Privacy by Design parameters are met. However, the fact that Privacy by Design principles are general and the legal scholarship still debates their practical adaptability and implementation, it may take a significant effort for these systems to be adopted.

One example that can be utilized is the concept of a 'smart- consent form', as an application directly related to data protection relationships between data subjects and data controllers (and processors). Such an application could ensure real-time compliance with all the GDPR requirements provided for the informed-consent form and the related data processing. Smart consent forms would represent an interactive CLS interface to empower data subjects with real-time compliance information and data processing management. Such a CL implementation would even reverse the data subjects' position from passive to active. Indeed, a smart-consent tool would be able to intervene directly on the smart-setting of the information form and, consequently, on the data processing. This solution may also be the case for data controllers' internal data processing management systems, which require records and log-registers for every data processing. A Computational Law system to support this activity would be beneficial to prevent any legal violation as well as to optimize compliance management.

3.3.2 Examples of Existing Computational Law Structures for Privacy

To some extent, embryos of Computational Law systems for privacy implementation are already in place. Much of the literature on the subject focuses on Privacy-enhancing technologies (PET) as a technical method for protecting data by allowing online users to protect the privacy of their personally identifiable information (PII).[64] PET solutions are provided to and handled by services or applications and exploit techniques to minimize possession of personal data without losing the functionality of an information system.

The goal of PET systems is to protect individual personal data and ensure that their information processing is transparent, confidential, and user centered. PETs aim to manage Data Protection requirements empowering users' control over PII and its effects. Such effects include implementing GDPR principles such as data minimization, anonymization, informed consent, and providing the opportunity to remotely audit policy enforcement and its compliance with the Privacy regulatory framework. The range of PET solutions includes improved accessibility, log-in ledgers, records, archives, and tracking transfers of data and related metadata.

In this realm of PET systems, there are many examples of Computational Law applications focused on resolving one or more of the described challenges. In general, PET solutions address issues such as

anonymization, obfuscation, identification, accessibility, consent-management, compliance checking and data sharing.

One example of a PET solution is Enigma. Enigma is a decentralized, blockchain-based, open-source protocol that allows a party to perform computations on encrypted data through smart contracts.[65] Enigma purports to turn ordinary smart contracts into "secret contracts," allowing developers to use a combination of cryptography-based technologies and hardware-based privacy techniques called Secure Multi-Party Computation (sMPC).

The idea that underpins this mechanism is that of dynamic privacy paradigms, in which data controllers' mining algorithms would access only the data that they absolutely needed, without connecting it to a specific individual's identity. SMPC tries to emulate a trusted third-party intermediator that stands between data subjects and data controllers. The system aims to provide a decentralized network of computers that will avoid data leaks during third parties' computation by dividing the information. Indeed, each computer in the network only sees encrypted bits of data without accessing the complete personal data.

Other examples of this mechanism are OpenPDS[66] and Opal[67] projects, which both adopt the same question-answer paradigm combined with both the disintermediation of data subjects' identity and the personal data fragmentation through different pieces of encrypted source codes. The same disintermediation paradigm is implemented for mediating data subjects' authentication, and authorization through the so-called Federated Authorization Framework (FAF),[68] which is an architecture that allows individuals to control their personal data with a scalable User Managed Access (UMA) protocol.[69]

Another important aspect to stress about the described Computational Law systems for Privacy is that they do not address the intimate difference between data and information. Data can be seen as containers or a units, which carry multiple pieces of discrete information. Recorded data represents the crystallization of information into a certain arbitrary category, while information is the ethereal set of characteristics, patterns, and elements that can describe things (objects, subjects, events). Therefore, data is the material representation of information, which serves to measure the discrete information and categorize it for interpretative means. In this sense, if a data controller can access only single data, it is not prevented to extract the relevant information that they carry and to infer patterns or other sensitive information. For instance, knowing only the timestamp of the last activity on a smartphone can convey information about sleeping. If a data controller can access a set of this data, such as the last usage in the day and the first usage in the morning for a week, they can easily infer sleeping habits and other sensitive data. This differentiation is crucial to define the capabilities and characteristics with which a CLS can be designed. Indeed, the CL system able to analyze only sets

of data would always need an external (human) intervention to interpret the information extracted by the aggregate data. On the other hand, depending on the CL architecture and its actual computational power, such a system may be able to perform a level of abstraction that could produce novel insights. This would render the system autonomous, consistent with the jurisprudence and self-executive because it could avoid external intervention/integration/validation, rely on the updated state of the courts' orientations and assess the compliance of a situation regarding the actual circumstances.

However, another problem these systems will have to face in order to achieve global adoption, is that their primary focus is on avoiding any identification. This can discourage data controllers from adhering to the system since there is a need to handle PII with appropriate care. This may also be a disincentive for uses because they lose any reputation benefits that are associated with not collecting the data.

At a broader level, however, these are all reasons that an approach to Privacy rooted in Computational Law is appealing. The described Computational Law structures can be implemented, reinvented, and refactored in light of the myriad Privacy frameworks that exist in a way that builds up a stronger global consensus about how to address these challenges. Indeed, if we design a system in a manner that requires third-party data controllers to specify the purpose of their requests for information, specifying how it will be used, and empowering individuals to track the usage of their data and revoke consent in different scenarios, a Computational Law architecture for Privacy would represent the perfect tool to shift the balance of power back to the individuals who are actually producing the data.

4.0 Limitations of Computational Law for Privacy

Given the current state of the art, a CLS could be sufficiently effective in the domain of privacy for managing compliance, auditing requests, and streamlining transactions. Nevertheless, the global nature of the internet, the ubiquity of data producing applications, and the promise of even more technological disruption requires a higher degree of artificial understanding. As shown above, a legal system is not the mere sum of isolated provisions that must be spell-checked. On the contrary, it is the exponential result of a complex interaction among different elements, which are diverse from each other as per their nature, scope, and effect. The law is more than just a set of articles. The provisions contained in one article must be read in reference to those explicitly or implicitly recalled in its concepts, and keeping in mind the underlying principles, structures, and limitations that inform some single norm. A legal system functions like a clock mechanism, in which every single element fits perfectly the wheels around and all together allow the right functioning of the system. So far, only the human mind is able to address this kind of complexity and provide a usable legal result in a timely manner.

For these reasons, in order to design a complete and efficient CL system, designers and developers must also take into account the current limitations that may undermine several architectural approaches. The CL structure is affected primarily by the aim it must achieve, and this influences the range of the outcomes. Therefore, it is important to be aware of the principal legal limitations to which CLS can incur because of the current state of technological capabilities.

4.1 Logic and Programming Language

As shown before, Legal Logic entails a level of nuance that is not so easily expressed in the simple binary logic of true/false, valid/invalid, applicable/non-applicable and just/unjust. And while it is possible to build a CL system which exploits the fuzzy logic to address the issue, the underlying specification issues remain. Fuzzy logic works as a values quantifier and not as a concept qualifier. Therefore, all those situations in which the complex legal phenomenon[70] involve potential outcomes that must be measured for their qualitative interrelations, a separate kind of computational approach is needed. It derives that a basic CL system with binary or fuzzy logic has limited applications when it comes to addressing these phenomena. These CLSs are valuable tools for simpler issues in which there is a case that only addresses the application of a single norm. For these cases, an *If-Then* logic is sufficient to guarantee the logical validity of the reasoning (but, in any case, not its truth). Alternatively, in more complex scenarios, fuzzy logic can be valuable to contemporarily address a set of related easy cases that refer to a common situation. An easy example of this in Data Protection can be found when making a determination about whether a consent form respects the requirements provided by Article 13,[71] the CL system only tests if the sample contains all the listed elements. It performs a quantitative binary analysis that checks the presence of the required element in the consent form. Fuzzy logic may help us if we address the issue considering some further detail, such as the purpose, that must be specific and must require a precise legal basis[72] for each purpose.

Nevertheless, if we want to investigate if the provided data subject's consent is valid, we must refer to the essential elements provided by GDPR Article 4(1) (11)[73] in order to consider freely given, unambiguous, specific and informed. The latter two elements can be solved with the fuzzy logic, as above, because the analysis entails a quantitative check. Instead, for the former two elements, it is necessary a qualitative analysis that cannot be solved with a quantifier. This requires a much more sophisticated analysis that evaluates the cross-references and the accepted interpretation of what is considered "free" and "unambiguous" consent. An AI-based CLS which relies on the so-called neural nets might serve the case. Artificial Neural Networks (ANN) are computational models composed of connected units (so-called artificial "neurons") that mimic the simplification of a biological neural network, such as the synapses in a biological brain.[74] Each connection can transmit a signal to other neurons which process the information and can relate to other neurons connected to it.[75]

On the left side of *Figure 2*, the output layer is represented by the blue neurons and works as a condition. In the given example, if the first red neuron represents the consent, and the first yellow one represents the correct information in the consent form, the blue neuron will be positive (compliant). This, however, is an oversimplification that applies only to the very first level of the easy case. Instead, in the qualitative example referred to the free and unambiguous consent, CL system should adopt a more complex scheme, on the right side of *Figure 2*, which represents the Deep Learning Neural Network.

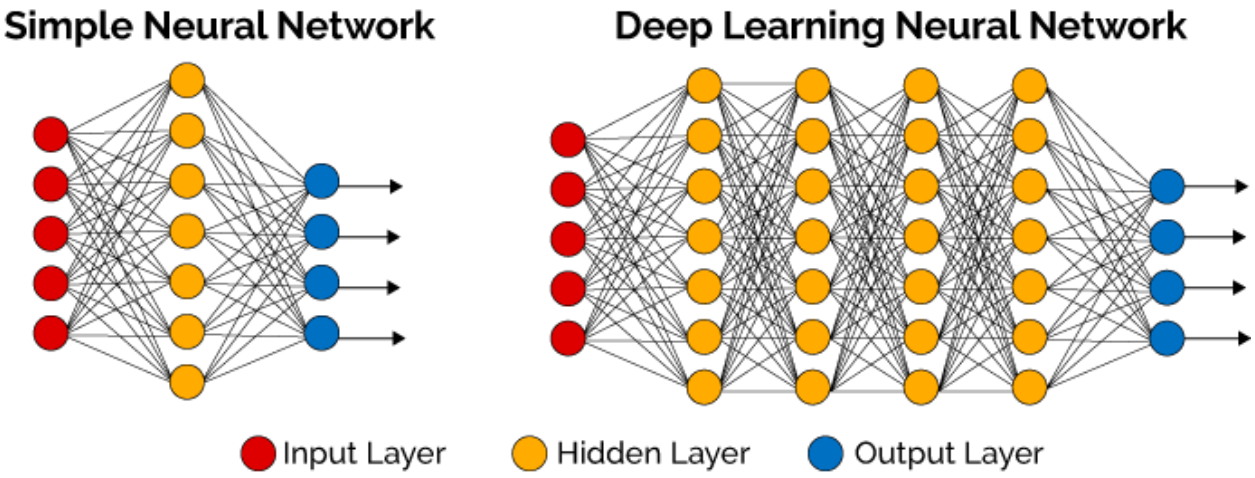


Figure 2[76]

Nonetheless, we are still in the realm of combined easy cases. When it comes to hard cases, we may encounter the real (current) limitations of CL systems. These limitations consist of both the computational power and the semantic level of the logical operators. The first would require too much computational power, energy and time to calculate all the possible solutions and outcomes, even exploiting the heuristic techniques[77]. The second refers to a set of hidden layers that may overlap, or formally represent the same concept but substantially refer to different ones. Many references may also be implicit in the norm or informed by principles provided in entirely different domains. Indeed, complicated cases are complicated not only because they hold a large number of possible acts, facts, effects, and implications, but also because they entail a background knowledge over the whole legal system of reference and all of the contrasting principles, rules, and provisions therein.

4.2 Language and Semantics

The reign of the Law is a human manifestation described by language. This means that any CLS that is fully integrated will require a similar level of complexity. In truth, the Law adopts only a specific linguistic register, which is the formal prescriptive proposition. Nevertheless, it is also formed by a technical jargon that is typically known as “legalese,” and this is used in legal interpretative reasoning, motivations, documents and agreements. The ontology of the specific language affects the ontology of

the specific legal system. Indeed, for instance, at a macro-level, Common Law systems formed and typically rely on English, while Civil Law systems on Romance languages instead. The differences in the structure of the system to some extent, reflect the structure of the language and its characteristics.[78]

If we consider the Civil Law, which typically has positive codification, even the different position of a term or punctuation can change the meaning of a precept. Words matter in the Law and their semantic meaning matters even more. Nevertheless, the semantic meaning of a word entails a realm of blurred concepts that can be overlapping, contrasting, or different depending on the given context. An extreme example can be the enantiosemy phenomenon, which involves that a word has multiple meanings, of which one is contrary to the other. For instance, the word “cleave” can mean "to cut apart" or "to bind together." Although this case is not so common in a preceptive proposition, the example can illustrate the level of complexity with which a CL system must deal with. Precisely, even a Deep Learning Neural Net system cannot address this level of complexity.

The current state of the art for speech interfaces gives empirical evidence for it and their linguistic limitations. The corresponding field that addresses this linguistic area from a computational perspective is appropriately called Computational Linguistics. Computational Linguistics addresses the semantic issues with a ruled-based, statistical approach to understanding language. One associated domain of Computational Linguistics is Semantic Computing, which seeks to combine elements of data mining, statistical analysis, natural language processing, and computation in order to better understand the structure, usage, and meaning of sentences. One challenge for these applications is the vast amount of labelled data that is required in order to achieve a high level of fidelity. Resultantly, these matters and their applications are still far from achieving a real general computational complexity that a whole legal system requires.

Some help in this domain may arrive from the Quantum computing realm, in which the qubit can address myriad combinations of 1 and 0 contemporarily. This means, by analogy, that quantum computing embraces the semantic form of a binary status. In this sense, qubits may represent an upgrade to the fuzzy logic toward, perhaps, a foggier logic. Indeed, the fog conceptual visualization represents accurately the ineffable nature of a word meaning concerning a specific context, which assumes a particular sense only when collapses into the hermeneutical measurement. The similitude attires precisely the nature of Quantum Mechanics and, in fact, in order to catch the whole semantic complexity of a complete legal phenomenon, a type of Quantum Computational Law may be required. The following Figure 4 illustrates properly the complexity given by the interaction of many foggy semantic concepts combined together, which is an accurate metaphoric representation of the interpretative complexity of a norm.

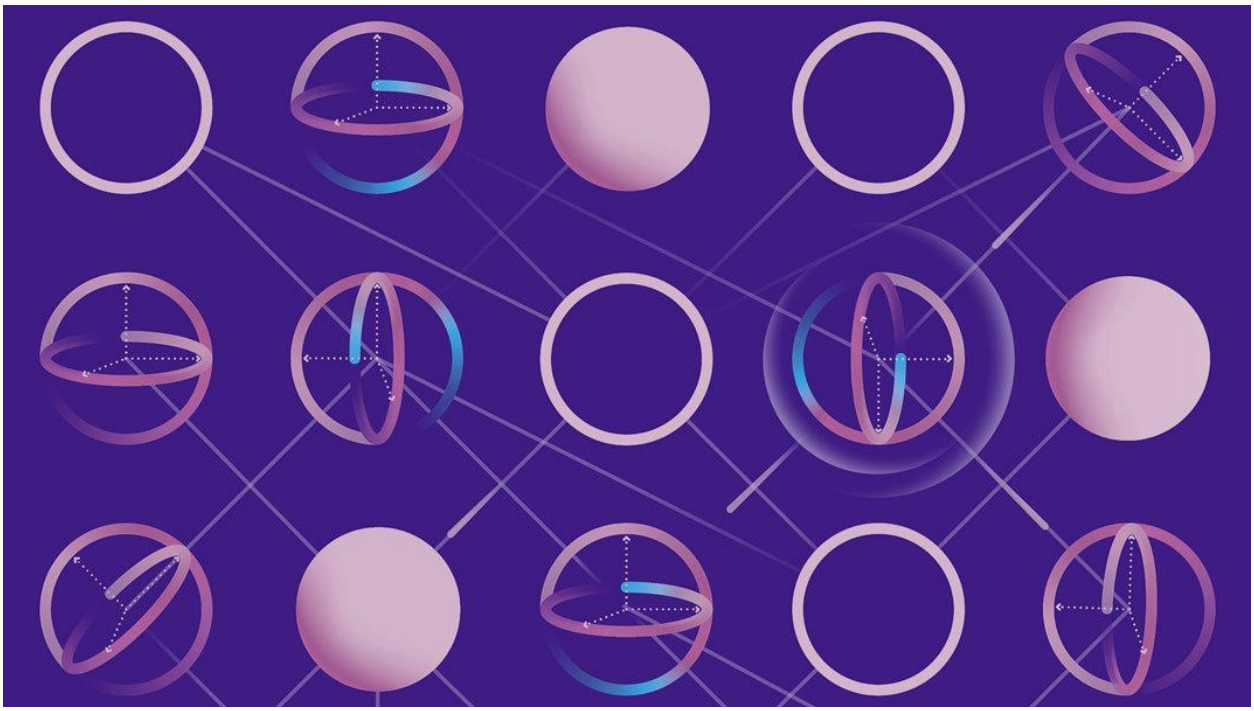


Figure 4[79]

4.3 Legal Dichotomies

Computational Law Systems must also deal with another set of issues, formed by the dualistic nature that composes the legal systems. We can refer to this nature as 'systemic dichotomy' when it involves procedural and substantive norms. We can refer to it as 'regulatory dichotomy' when it involves rules and principles. These dichotomies affect the applicability of CL systems, as the latter can currently work efficiently only for, respectively, procedures and rules. Indeed, procedures are nothing else than a set of instructions. Even if they can entail several sub-layers substantive precepts and the related semantic issues, their primary structure relies on commands that can be translated into binary or fuzzy logic inputs. The same goes with rules, which are finite precepts, i.e. typically either commandments of to do, or not to do something or provisions upon certain requested characteristics. For rules, however, the general limitations described in earlier remain valid. Indeed, they can be either procedural or substantial. The complexity increases when rules start to encompass conditions or cross-references.

On the other hand, substantive norms and principles are subjected to all those limitations already described. Substantive norms can be descriptive and prescriptive. When they describe a general right, they do not provide any command other than the implicit one of recognizing all those situations that fall into that general description as per that particular legal category. Therefore, a norm provides a descriptive proposition when it describes the general characteristics and lists the conditions of a situation, such as, for instance:

> *"The owner has the right to enjoy and dispose of things in full and exclusive, within the limits and with the observance of the obligations established by the legal system"*[80].

To some extent, this descriptive proposition can be translated into machine-readable code, as the set of characteristics and conditions. However, when it comes to interpret what "enjoying" and "dispositions" imply, the CLS cannot deal with the substantial norm without dealing with the semantic cross-reference, as above mentioned.

Finally, at a conceptual level, principles are foggier than the norms and cannot be measured or condensed into finite characteristics or conditions. Their nature is as general as it is abstract and may be adapted for many subjects in many situations. In a particular context, the principle can be applied. However, in broader contexts, it is much more difficult for a computational system to deal with principles. Indeed, even if a hypothetical CLS was able to address all these ethereal nuances by understanding the complete collection of case-law, jurisprudential decisions, and doctrinal opinions, it would need to be able to weigh any potential conflicts with the principle in light of moral values. For instance, in a controversy in which two fundamental principles[81] conflict, the system would need a deeper understanding of the ethical considerations, in addition to only the legal considerations.

4.4 Programming Bias

CLSs must be coded in order to perform their task. Coding is not a neutral action but requires explicit or implicit decisions. First of all, developers must translate the legal (human) language of the norm into the programming language. "Ergo" is one particular programming language developed exactly for CL systems (specifically smart contracts).[82] Its syntax is designed to serve the specific needs of a legal contract, in order to avoid run-time errors and non-terminating logic.[83] Nonetheless, as every human-created language, it is arbitrary and might entail several forms of bias. For instance, if anglophone developers created the programming language, it may refer to the Common Law system legal approach. It may also be the opposite. However, as Common Law system is based on case-law, if the programmers did not consider a particular situation, that situation might remain overlooked. However, it would be difficult to create a programming language that adhered to both Common Law and Civil Law approaches, as each uses a different vernacular. For instance, it may be hard to interchange the two and apply one partisan programming language to the opposite system. At the very least, it would be foreseeable that ontological mistakes would arise and start to undermine the scope of a Computational Law system. Even at a conceptual level, the notion of a neutral programming-language cannot exist. The structures of the language necessarily inform the outcomes of a system reliant upon that language.

The same kind of bias can affect the coding on a level of bias. This is apparent when the programmer exploits the language to encode a particular set of legal instructions. For instance, if developers

address the European Data Protection regime and encode the instructions with the US subsumption that personal data represents a property, and the data subjects own their data, they create an inconsistent legal framework. This situation can easily become a bug or, worse, an exponential error that undermines the results offered by the system.

On a third level, programmers should also be aware of the unlawful (or just incorrect) legal parameters that they may incorporate into the system. Indeed, if in a smart contract the programmer establishes a certain effect upon the occurrence of certain conditions, he must be sure that both the effect and conditions are lawful, valid, applicable and enforceable. Therefore, in order for a programmer to be optimally effective, they should effectively be able to translate the legal matter into code in the first place and be accountable for any mistake.[84]

4.5 Interoperability

In order to be widely effective, a CL system must be interoperable among different jurisdictions. Indeed, we must consider that CLSs will not be merely based on local regulations. Global transactions require common legal ground, be it Merchant law, conventional national law agreed by the parties or International Private law. Even if the system's application remained into the national border of one jurisdiction, it would have to deal with different subsystems at the same time. This implies not only the classical hierarchical level and the vertical axes[85] but also the different laws for each state/region/department and each town/area on the horizontal axis. This level of granularity requires the system to coordinate all the different regulations in their hierarchical model, managing the so-called apparent conflicts between the laws.[86] The same kind of interoperability must be granted on the level of Civil and Common Law when the application requires such an interaction. This is the case of the GDPR compliance within the United States for those services that fall into the territorial and material scope of this EU regulation.[87]

Jurisdiction itself is another important aspect with which the system must deal. In the Common Law, the English term "jurisdiction" actually refers to two different concepts that in Civil Law are named separately. One is the so-called "competence", and the other is precisely the jurisdiction. The former refers in general to the sphere of powers and entitlement attributed to specific subjects. In particular, it refers to the material sphere on which a judge can decide or not a controversy, depending on the matter[88] or the value[89] of the issue. Jurisdiction refers instead to the State and its organs (judges) authority to decide over a certain matter in relation to a specific territory. The CLS must comprehend and harmonize in its functioning both the concepts and what they bring in terms of legal outcomes. This also implies that languages too must be harmonized by the system. Even if the programming language is the same, different languages imply different semantics and shades. In turn, this would

also imply potential language biases for the system as well as language bias and limitations for the programmers.

Moreover, the system must also grant an interactive dynamic reference to the changing laws. Indeed, legal systems are far from being static, and the laws continually change, because of modifications, integrations, amendments, deletions, or repealings. The law itself is made by dynamic reference. Indeed, if law X makes a reference to an article Y in the law Z, and successively the article Y in law Z is modified, law X will be modified consequently. The modification will occur immediately and to the extent of article Y impact over the law X effects, and even if the law X has not been touched by any amendment directly (a sort of legal entanglement). The Computational Law system must be resilient to these changes and, besides, be able to welcome them in real-time and to highlight the change if it is the case.

4.6 Interpretation and Explainability

Understanding the role of interpretation with regard to the integration between a CLS and a traditional legal system presents another challenge. Legal Logic forms the cornerstone of all legal argumentation, which can be broken down into single components of the norm as well as of the legal situation. In order to do it, it is vital to evaluate properly all the ingredients that compose the legal scenario: regulatory system and its hierarchy, the case-law, its subjects and related legal status and the norms that apply to the situation. The regulatory system is the term of reference, as all the interpretations must conform to its principles and general rules. The "case" is the set of acts and facts, as generated or undergone by subjects involved, of which only the legal acts and facts compose the legal situation, i.e. the set of elements addressed abstractly by the Law. The norms are the specific precepts that apply to the case, singularly or interaction with one other.[90]

When considering the norm, the interpretation must focus on the prescriptive proposition and its structure. Grammatically speaking, the proposition is composed of a subject and a predicate, but the proposition must be distinguished from the grammatical statement. The latter is a linguistic form in which a specific meaning is expressed. Therefore, the same proposition can have different statements, and the same statement can mean different things in particular contexts.[91] Also, the meaning is essential because it explains what the norm aims to prescript and because it must be coherent with the whole system. Indeed, the normative proposition might be formally right, but not valid, unjust or inapplicable.

The interpretation aims at foreseeing the right effect that the consistent application of the norms will entail. As mentioned before, the legal system must provide certainty, and this scope is achieved thanks to the coherence among all the norms and the fundamental principles that inform the system. Therefore, the principle of coherence is the link between the logic and the prescriptive proposition and

should avoid the rise of conflicts among the norms. Nevertheless, many apparent conflicts may occur during a formal interpretation, and the system provides with hermeneutical tools to solve them: hierarchy, chronology, and speciality.[92] Interpretation also relies primarily on the use of legal syllogism and both the deductive and inductive reasoning. In turn, the deductive method is a cognitive process that moves from the general to the particular (top-down approach) by extracting a logical (coherent) conclusion starting from at least two general propositions considered true. It applies to the analysis of the norm. On the contrary, the inductive method is the process that moves from the particular to the general (bottom-up approach) and produces a general conclusion starting from two facts. It applies to the case law analysis.

As the meaning is pivotal in the prescriptive proposition, the interpreter must deal with the literal analysis of the norm and the literal meaning of every word. Semantic plays an essential role because it is not always easy to understand the exact meaning of a particular word in a particular context. Legal semantics must be understood as per the grammar positioning of the word (logical analysis of the predicate), as per the punctuation and different predicates of the proposition, and as per the accepted meaning in both the body of norms, the jurisprudence and the doctrine.[93]

As the norms are not motivated, the interpreter must conduct a formal investigation over the norm. The first analysis invests the scope of the norm, i.e. the kind of prescriptions that it literally states. Then, it addresses the position of the norm in the system (positioning) and the relation of the norm with its regime of reference (systematic analysis).[94] With this in mind, the analysis moves to the evaluation of conditions and presumptions. The condition deals with the set of elements that constitute the necessary assumptions for the application of the norm. For instance, legal statuses[95] are preconditions. Presumptions instead represent a legal fiction aimed at ensuring the certainty that the system must provide to the subjects of law. Indeed, many social situations must be hard to prove or disprove, and so the Law establishes that if certain conditions apply, a situation must be considered in a certain way unless it is proved differently. Furthermore, when analyzing the fact in reference to the norms that govern it, the interpreter must also consider the cause-effect etiological relationships between acts and facts and its factual or legal imputability to the subject. The Law focuses on effects, and the conduct serves residually to an ex-ante evaluation over the degree of possible negligence concerning the cause-effect occurrence, which constitutes the legal fact. The last step in the formal investigation of the norm addresses the protected good, that is the legal good that is the object of the protection.[96] It must not be misunderstood with the object of the prescription. Indeed, for instance, in the norm “vehicles must stop when the traffic light is red” the object of the prescription are the vehicles and the protected good is the road safety. As seen, the meaning of a term might be obscure or unclear: for instance, ‘vehicles’ may refer only to motorized cars, because its semantic is narrowed by the context or by the legal subsumptions. When the interpreters cannot find clues in the regime of

reference, they can perform the so-called psychological analysis, meaning the legislator's intention, by investigating the memories and notes over the preparation of the law, in order to understand what the legislator[97] aimed to protect or to refer. Other tools are 'combined reading' and 'legal analogy.' The first is a technique of semantic interrelations among norms of the same legal regime. The second is a residual technique that searches for common elements in other legal situations and the respective regime.[98] The scholastic example for it is that when airplanes were invented, courts borrowed the legal regime for navigation.

As seen, predictive analysis and structured classification are core elements of the formalistic legal interpretation. For this reason, on the one hand, the contribution of CLS to the structural analysis of a situation can be relevant, and, on the other hand, this body of structured data can be practically encoded into machine-readable systems. Nevertheless, there are many unstructured variables that may undermine the productive outcome of a CLS in an in-depth interpretative analysis of a hard case. Indeed, what Dialectic, Rhetoric, and interpretation have in common is that they all tend to pursue a structural justification for the legal argument. The reason for this scope must be found in the ambiguity of the norm, which is abstract and not motivated. Besides, the decision over a case must be motivated by the Judge according to the principle of reasonability, as the scrutiny on the normative application cannot be arbitrary but must be coherent with those same principles that inform the norm. This is why Dialect and Rhetoric aim at argumentative persuasion. Nor the prescriptive proposition, neither the private autonomy in performing legal transactions must be motivated, and this renders complex the interpretation of norms and legal situations. The interpretation aims at finding the presumptive motivation and prove or disprove that the best rule is applied to the case.

However, the need for an explanatory justification over the reasoning might complicate the application of Computational Law to the interpretative system. Indeed, CLSs are software-based analytical tools which more and more will rely on AI infrastructures as machine learning, deep learning and neural nets. One of the current main issues related to it is the "black-box" problem, namely the incapability of AIs to explain the motivation behind a choice or an outcome. If this is the case for CL systems too, this can be a practical obstacle to the automated interpretative application of the Law.

5.0 Quantum Law as a possible solution for advanced Computational Law Systems

As shown above, CL systems must deal with several limitations. The semantic ontology of the technical language required by law and the conceptual complexity therein represent obstacles that the current AI state of the art is not able to overcome.[99] For the time being, CL systems may appear to be relegated to a narrow class of applications, focused on cases or applications that are limited in terms of their complexity. However, drawing analogical inspiration from the field of quantum mechanics can help us

to imagine a conceptualization of the fundamental elements of law that is capable of addressing equally complex phenomena - Quantum Law.[100]

Quantum Mechanics is the discipline that studies the behavior of subatomic particles[101] and, if applied to the Law with a thought experiment, it would address fundamental elements such as single norms, or principles, as sub-situational essential elements or particles. At first glance, law and quantum physics would seem to be far apart from one another. However, both systems describe and measure the behavior of elements. Indeed, the Law's scope is to provide certainty and stability to human relationships and, above all, to their effects, in order to ensure their foreseeability. Unfortunately, however, the predictability of particular legal outcomes is far from being absolute because many different unforeseeable variables play a role in their determination. We may argue that knowing all the variables would empower us to calculate a precise legal outcome with a deterministic approach, ensuring a total predictable output. Yet, even though the legal system is finite and made of rules and instructions, the variables that interact in a legal situation do not work in a deterministic way. This is because the system encompasses the realm of semantic as well as of human behavior, which cannot be bridled into specific deterministic descriptions.[102]

Indeed, the Quantum analogy was already investigated for the Law as well as for other fields, by some author in relation to specific doctrines[103], disciplines[104], or domains.[105] In these works, the Quantum metaphor is used to describe common features and better understand the nature of the topic addressed. To some extent, these works each recognize that the Heisenberg Indeterminacy Principle applies to some features of legal situations.[106]

Here we introduce the seed of a new theory for the Law, i.e. 'Quantum Law', which aims at demonstrating how the Quantum Mechanics principles can be applied fruitfully to legal systems. Specific attention to frame it, is paid to Civil Law systems. The aim of these efforts is to show that the practical application of Quantum theory to sub-situational legal phenomena can help in predicting the legal outcome of an observed, complicated legal situation thanks to a quantum-probabilistic approach.[107] Specifically, this epistemological interrelation serves to highlight the practical usability of this theory for Computational Law systems.

If we address the Law in its general terms, we can already start seeing some analogy with the Quantum realm. What lies between an act or a fact and its effect (i.e. the subject's behavior) remains to some extent obscure. Indeed, it can only be reconstructed ex-post and through the limited tools allowed by the system (the legal evidence). This fact shows that every legal situation remains abstract and undetermined until it is measured (interpreted or applied). For instance, we statistically breach some law every day. We unwittingly perform some illicit acts on a regular basis, including illegally

crossing a street or violating the terms of use of a website. This behavior can be punished only to the extent in which it is detected, reconstructed, and measured (i.e., judged).

Any attempt to measure a legal phenomenon implies the 'collapse' of the elements into a specific legal result, which was unclear and unpredictable before the observation. Consider, for instance, a trial and the judge's room for maneuver in interpreting the whole legal situation and the set of norms and principles that interact with it. Therefore, the judgment is the paradigmatic measurement of the applicability of an abstract norm to a measured phenomenon. When a judge decides the actual and exact application of a single norm (i.e., our particle in the Quantum analogy) to the case-law, they crystallise the probabilistic outcome of a legal interpretation into a precise legal output. Not only that, but by interacting with the situation, the judge influences the situation itself (the effects) and the structure (behavior) of the system.[108]

In fact, the norm is the fundamental element that constitutes the legal system. It can be seen exactly as an elementary particle, which is no further divisible in its preceptive principle. One must note that a norm is not an article. An article can hold several norms. Also, a norm is not a rule: the rule is a particular kind of norm, which expresses some instruction and may also entail a set of connected rules. The norm is instead an essential precept. Not to be misunderstood is that the norm, as a concept, differs from the text by which the norm is represented, which of course is divisible. The text of a norm can be different, while the precept remains the same and vice-versa[109]. Indeed, the text is a characteristic of the norm. On the same line, every further connotation that a norm can have, such as descriptive rather than prescriptive or conditioned rather than general, constitutes a particular characteristic of the norm and this is in line with the characteristics that particles can present in a Quantum reality.

Using this inspiration, norms are quantic by analogy. That is, they are finite but carry a variable amount of legal instructions that can range on a particular spectrum (frequency) depending on the type of information that it carries. Like a photon, this frequency depends on the color frequency (the legal characteristic) that it carries. It can be in the visible spectrum, meaning those norms provided positively by the systems; or it can move in the invisible spectrum, ranging from legal principles to social and ethical norms.

Further, the norm can be seen as holding a dualistic nature, exactly as the quantum counterparties. It behaves like a corpuscle when collapsed into a precise application, and it behaves like a wave when it is not detected. The norm's wave represents the semantic oscillation of its meaning in different legal scenarios. In this case, we can see its effects but cannot check its real position (applicative meaning) in a specific scenario until we measure it. This legal wave propagates toward space (and time), which is represented by the set of relationships among different elements of the system of reference.

Therefore, according to this analogy, the norm is not the only particle in the quantum legal realm. Many other elementary legal elements present the same sub-situational quantic nature as the norm does. The legal subjects[110], the legal acts, the legal facts[111], principles, rights, duties, and interests are among these elementary particles.

One particular fundamental particle that competes with the norm in terms of importance is data. As seen with the difference between 'data' and 'information', data can also be seen as ontologically quantic: it is a unit that carries a certain indefinite amount of information. For instance, the name "Gianluigi" is a data but conveys a set of variable and indeterminate[112] information: it is a name; it is the name of a human; it is a name of a man; it is a name from Italy; it is a double name. However, this information is indeterminate and fluctuates like a wave, because if we do not measure the data in the reference system, we cannot be sure about the extent of validity of the aggregate information. For instance, observing the particular case-situation, we might discover that it refers to the name of an American female pet which is actually called by the owners with the nickname "Gian."

Indeed, only a few pieces of the information carried in the wave corresponds to a determinate state when collapsed (observed). In turn, data can be personal or non-personal. This is one of the characteristics of the particle. When data is personal, it falls in the privacy particle. When data is non-personal, it falls in other legal-quantum domains, such as trade secrets or copyrights. However, it is important to note that all of those fundamental particles behave according to the same scheme that reflects the concepts and mechanisms of Quantum Physics.
One simple deduction that can be carried out from the analogy is that if the legal system appears to behave like Quantum Mechanics systems, it can also be described and measured according to the same analogical criteria and laws. This must be seen as the cornerstone of the Quantum Law analogy, as it defines the exact scope of the thought experiment and connects the Computational Law systems limitations and implementations for Privacy, in order to reach interpretative legal solutions.

The hypothesis that we highlight is that if the legal system analogically reflects the Quantum Realm or at least some of its characteristics, it could be addressed with the same type of approach. For example, if a norm's behavior in a trial is understood according to Quantum Mechanics' wave function paradigms, its correct potential interpretation could be determined in a quantic-probabilistic way. This would be the eventual benefit for fully integrated Computational Law systems, which could combine this probabilistic mathematical analysis of the norm with the overall fuzzy logic that governs the whole phenomenon analysis. Indeed, we should keep in mind that the Law is made of language and it is performed through living actors. In this sense, several studies already showed how Quantum laws can be applied to many branches of different domains that go from Quantum cognition,[113] to Probabilistic logic,[114] Probabilistic semantics,[115] and Probabilistic decision-making.[116] From this analogical viewpoint, there is evidence that the legal system analogically mirrors the Quantum Realm.

The practical application of this quantic legal knowledge stands to benefit the design of increasingly complex Computational Law systems. Simple algorithms are already used to measure contract performance. Further, into the future, probabilistic functions and equations can be increasingly expressed in a machine-readable, mathematical language. CL systems could exploit Quantum Law to calculate the probabilistic nature or behavior of a particular norm in a precise legal situation and space, in order to determine its plausible concrete probabilistic application and combine the result with the overall high-level computational analysis of the whole legal phenomenon addressed. In this way, CLS would not have to 'understand' the law in order to reach a proper interpretation but only would need to calculate it based on a set of Quantum probabilities. Then such a system could be adapted, evaluated, and discussed in order to fine-tune the Quantum approach to the concept of "lawfulness" in a particular legal system. Nevertheless, this theoretical framework requires prototyping, testing, and evaluation before it will be possible to more concretely examine the strengths and weaknesses of these applications.

6.0 Conclusion

This investigation tackled the topic of Computational Law systems and their implications for Law and Privacy. It afforded the challenge to analyze the Computational Law applicative phenomena as a whole, considering the interactive elements that contribute to its implications and potential developments, as well as its limitations. The focus of the study was to investigate how the issues, limitations, applications and implications of CL systems interact with the Privacy realm. In order to properly argue over these topics, the study first drove the readers through some necessary concepts related to the background of technology and the Law. Specifically, the work outlined the concurring technologies for the Computational Law ecosystem and how they work, especially considering the forthcoming wave of Internet of Things devices. The study provided the readers with a comparative analysis between the effects of existing regulations for Privacy and Data Protection in the context of the US and the EU.

The study then evaluated the notion of computational law as a partial solution to existing privacy issues, with specific attention focused on Privacy by Design and emergent tools for regulating Privacy. However, even these sophisticated approaches may be inhibited by the future development of new technologies such as Brain-Computer Interfaces. To account for the increasingly complex legal challenges that we face, the notion of Quantum Law was offered to show how these solutions might eventually fill interpretive gaps in legal contexts by ensuring an external human help to the machine's cognitive limits or with an applicative solution at the intersection between the Law and Physics. Here the work posited the ground for Quantum Law analogy as a parallel conceptual representation of Quantum Mechanics. This paper then argues why this approach could eventually fill the gap of the

Computational Law systems' interpretative limitations, by adopting a probabilistic analysis of the specific interpretation and application of the norm in a precise legal situation.

The paper provides an original contribution on many fronts, by exploring the holistic connections of the central theme - Computational Law and Privacy – through an interdisciplinary big-picture oriented analysis. It opens many lines of discussions that can be investigated in future works. Indeed, the paper introduces the challenge of exploring the Computational Law system applicative limitations in relation to the different legal systems. It also provides the essential elements to deepen the study of blockchain and smart contracts concerning privacy rights and Data Protection requirements as well as the benefits for Privacy by Design and by Default of implementing real-time CL self-management tools such as 'smart consent-forms'. Furthermore, the work connects new technologies such as speech interfaces (smart speakers), BCI and IoT ecosystem with Computational Law applications and their implications. The paper also paves the ground for the investigation of a new interdisciplinary conception that stands at the edge between Law and Quantum Mechanics, and that could have many potential applications in both Computer Science and legal matters.

In conclusion, the investigation draws a line on the whole potentiality spectrum as well as on broad limitations of Computational Law systems and their relations with the Privacy realm. It highlights how important it is to consider this matter with a broad approach, especially to overpass the practical and conceptual limits that the current and future applications of Computational Law imply.

Gianluigi M. Riva is an affiliate of School of Information and Communication Studies, University College Dublin. gianluigi.riva@ucd.ie and a Fulbright-Shuman Visiting Researcher at MIT Media Lab, Human Dynamics group, at Massachusetts Institute of Technology

---

Acknowledgement

This investigation has been carried out thanks to Fulbright-Shuman Grant scheme for Visiting Research Projects

Footnotes

1. Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/ (last visited Nov. 25, 2019). ↩
2. GDPR Article 17. ↩

3. Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union L 119/1. ↩
4. See e.g., Issie Lapowsky, "How Cambridge Analytica Sparked the Great Privacy Awakening" Wired, March 317, 2019. Available at: https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/ (last visited Dec. 14, 2019). ↩
5. See e.g., "FTC Press Conference on Equifax Settlement" Federal Trade Commission Media Resources Library, July 22, 2019. Available at: https://www.ftc.gov/news-events/audio-video/video/ftc-press-conference-equifax-settlement (last visited Dec. 14, 2019). ↩
6. See e.g., Megan Rose Dickey, "FriendFinder Networks hack reportedly exposed over 412 million accounts" TechCrunch, November 13, 2016. Available at: https://techcrunch.com/2016/11/13/friendfinder-hack-412-million-accounts-breached/ (last visited Dec. 14, 2019). ↩
7. See e.g., Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government" Wired, October 23, 2016. Available at: https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/ (last visited Dec. 14, 2019). ↩
8. See e.g., Daisuke Wakabayashi, Adam Satariano "Google to Buy Fitbit for $2.1 Billion" New York Times, November 1, 2019. Available at: https://www.nytimes.com/2019/11/01/technology/google-fitbit.html; Erin Brodwin, "DNA-testing company 23andMe has signed a $300 million deal with a drug giant. Here's how to delete your data if that freaks you out." Business Insider, July 25, 2018. Available at: https://www.businessinsider.com/dna-testing-delete-your-data-23andme-ancestry-2018-7 (last visited Dec. 14, 2019). ↩
9. EPRS | European Parliamentary Research Service, Panel for the Future of Science and Technology, *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?* At https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf (last visited Dec. 14, 2019). ↩
10. GDPR Article 22. ↩
11. For example, the Dark Web, Artificial Intelligence, and Human Augmentation. ↩
12. Ryan Calo, Privacy Law's Indeterminacy (November 8, 2018). 20 Theoretical Inquiries L. (2019). Available at SSRN: https://ssrn.com/abstract=3281159. ↩

13. *See e.g.,* Larry Lessig, *Code v2*, Basic Books, 2006. Available at: http://codev2.cc/. ↩
14. Alex 'Sandy' Pentland, "A Perspective on Legal Algorithms" MIT Computational Law Report, 2019. Available at: https://law.mit.edu/pub/aperspectiveonlegalalgorithms ↩
15. A.k.a. Smart Speakers, Digital/Virtual Assistants, Conversational Agents, Intelligent Vocal Interfaces and so on. ↩
16. Hassan Takabi, et. al., *Brain Computer Interface (BCI) Applications: Privacy Threats and Countermeasures*, 2016 IEEE 2nd International Conference on Collaboration and Internet Computing. ↩
17. Each country has different layer of regulations (national, federal, regional, local and so forth) and different structural organization. The granularity of these different regulatory frameworks would appear to suggest that an efficient CLS should also consider the normative hierarchies in each system of reference. Then, they should be able to interact with each other. Therefore, an 'efficient', or at least complete, CLS should be designed around one of these two legal systems. Only, in this case, there could not be interoperability between the different systems and CLS efficacy would be circumscribed to local applications merely. ↩
18. A global CLS may be utopic – at least at the moment – as much as the so-called 'general-AI' appears to be in the short run. Nevertheless, if CL aspires to manage the majority of legal-virtual relationships toward the simplification of automated processes, the possible current solutions are only two: either it serves only local jurisdictions, or it follows the International Private Law path relying on inter-jurisdiction legal mechanisms. *See* Fabrizio Cafaggi, *New Foundations of Transnational Private Regulation*, **J. of L. and Society**, 38, 1, Special Issue: The Challenge of Transnational Private Regulation: Conceptual and Constitutional Debates, 20-41, (2011). ↩
19. i.e. Smart Contract for international transaction that, therefore, work according to International Private Law (IPL) regulations, treaties and uses. Therefore, smart contracts performed between international parties should adhere to IPL provisions as chosen by the parties. CLS that enable international smart contracts (IPL based) to run, should consequently embed IPL frameworks and harmonize their functioning according to the legal regime of reference (i.e., those chosen by the parties). ↩
20. In International Private Law, the technique of choosing a precise jurisdiction that would decide over a contractual controversy. ↩
21. In International Private Law, the technique of choosing a precise Law system (national jurisdiction) that governs the contract with its national regulations. ↩

22. In International Private Law, the technique of assigning specific clauses to the rule of precise national laws other than the principal one that governs the whole contract. ↩
23. Cf. Stefan Vogenauer, Jan Kleinheisterkamp, eds., **Commentary on the UNIDROIT Principles of International Commercial Contracts (PICC)**, Oxford University Press, Oxford, UK (2009). ↩
24. That is, based on individual rights and self-determination. ↩
25. The US system relies on a Common Law tradition, in which the precedent rules and, usually, bind the court's decision according to the court's hierarchy -namely the so-called stare decisis. *See* Cf. HOWARD ABADINSKY, **LAW AND JUSTICE: AN INTRODUCTION TO THE AMERICAN LEGAL SYSTEM**, Fourth Edition, Nelson-Hall Publishers, Chicago (1998). The US system does not know the continental General Theory of the Law and the related rights categorization [See NORBERTO BOBBIO, **Teoria Generale del Diritto**, collana Recta Ratio, G. Giappichelli ed., Torino (1993).] Therefore, Civil Law's legal personality rights are called in the US Common Law system 'publicity rights'(name, image, likeness, privacy) and falls into the realm of Tort law (and parallel Prosser's "Four Torts") specifically into the tort of "passing of", such trademarks regime does. [See Judge Jerome Frank in 1953. *Haelan Laboratories, Inc. v. Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953). https://law.justia.com/cases/federal/appellate-courts/F2/202/866/216744/ (last visited Dec. 14, 2019).] In the US system Publicity rights are generally considered as a property right as opposed to a personal right, and as such, it can be commercialized through contracts. This is the manifestation of publicity as the right of an individual to control the commercial use of its property. The US jurisprudence (Legal Theory) justifies this kind of notion of natural rights with the idea that every individual should have a right to control how their right of publicity is commercialized by a third party. Also, US Tort law has punitive damages for liable parties. Overall, the US Contract law system is governed by the proprietary paradigm as the maximum expression of one's freedom and, accordingly, any breach of the right involves liability. Indeed, any violation of a right of publicity closely aligns with appropriation. Vice versa, the EU system is based on the Civil (Roman) Law tradition governed by the written statues (legislation and codification) which are constantly updated and in which precedents are not binding, but only persuasive *See* Cf. TYMEN J. VAN DER PLOEG, **A Comparative Legal Analysis of Foundations**, In: Anheier H.K., Toepler S. (eds) Private Funds, Public Purpose. Nonprofit and Civil Society Studies (An International Multidisciplinary Series). Springer, Boston, MA, (1999); And Cf. Geoffrey, C. Hazard Jr., *Discovery and the Role of the Judge in Civil Law Jurisdictions*, **Notre Dame L. Rev.** 73, 1017 (1997-1998).] Civil Law countries conceptually proceed from abstractions, formulates general principles, and distinguishes substantive rules from procedural rules. The main feature of Civil Law systems is that legal codes are designed with brief legal texts for their articles that typically avoid factually specific scenarios, dealing with general situations. This stands in contrast with statutory systems, which are often very long and detailed, as

they aim to rule specific matters. The General Theory of the Law informs the general characteristics of the Civil Law system: laws must be general, i.e. embracing the most of individuals possible, and abstract, i.e. embracing the most of situation possible; the conflicts among the laws must be resolved according to the criteria of chronology, hierarchy and specialization ; the conflicts among the principles must be resolved according to prevailing interests. All the legal items (subjects, objects, goods, and rights) belong to doctrinal categorizations, and thus, for instance, interests can be individual or collective, private or public, legitimate or not, lawful or not, and so forth. Rights are categorized too, and legal personality does not belong to Tort law and proprietary paradigm, on contrary to US approach. It means that individuals cannot commercialize these rights, but only licensee exploitation rights over them and the exploitation always undergoes the limits of fundamental rights and principles, as well as general principles of public order and morality. Fundamentally, for Civil Law systems, property rights can be owned only on material goods. Immaterial goods only can be managed with disposition rights. For this reason, they are typically unalienable, and some of them are unavailable or quasi-available. This structure has convenient effects: contracts can be affected by nullity or invalidity if parties do not follow these principles, and the individual consent is relevant only to the extent of the circumstances and in the limits of the room for maneuver permitted by the law (to protect weaker parties). For instance, consumers' contractual consent does not count on vexatious clauses, which are considered singularly null because against the law. These classifications are essential to understand Privacy and Data Protection in the different legal systems and to evaluate which effects CL can have on one or another approach. Also, CL seems to better adapt to the Civil Law system, as it is structured upon classifications, categorizations and written codifications that is literally interpreted, meaning structured data that would better fit a machine-readable mechanism. Common-Law system, instead, provides more ground for unspecified normative considerations. However, paradoxically, Civil Law system provides less certainty over a decision on a controversy, given the space accorded to the judge's interpretative power, whereas Common Law can ensure more foreseeability on situations that fall precisely into the parameters of a precedent. ↩

26. Paul M. Schwartz, *The EU-U.S. Privacy collision: a turn to institutions and procedure*, **Harvard Law Review**, 126, 7, 1966-2009 (2013). ↩

27. Among the many, the principle of consent, of information, of purpose, of necessity, of minimization, and so forth. ↩

28. In Civil Law legalese, "typic" is a rigid and close list of elements, which does not allow to consider any other element that is not listed. ↩

29. The EU paradigm relies instead on the 'rights entitlement' (over data), meaning that the data subject has subjective positions over his personal data, which are protected by a set of rights of

which he can dispose according to the limits drawn by the law. ↩

30. Consent must be informed, unambiguous, freely given and specific in order to be valid. Cf. GDPR Article 7. ↩

31. Cf. GDPR Article 6(1) a) and 5(1) a). ↩

32. GDPR Article 8. ↩

33. Gergely Csech, Renata Zelina, *General and Labor Law aspects of the GDPR*, **European Integration Studies**, 14, 1, 2018, at 102-110 ↩

34. Directive (EU) 2011/83 of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. ↩

35. In 1979, in *Smith v. Maryland*, the US Court affirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." ↩

36. For example, 1) Intrusion upon physical solitude; 2) public disclosure of private facts; 3) depiction in a false light; and 4) appropriation of name and likeness. *See* Beebe, Barton; Cotter, Thomas; Lemley, Mark; Menell, Peter; Merges, Robert *Trademarks, Unfair Competition, and Business Torts*. Aspen Publishers (2011) ISBN 978-0-73558877-6. Cf. with W. Prosser, *Privacy*, in California Law Review, vol. 48, (1960). ↩

37. See GDPR Article 32. ↩

38. Privacy Act of 1974, Pub.L. 93–579, 88 Stat. 1896, 5 U.S.C. § 552a; (1974), https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf and https://www.law.cornell.edu/uscode/text/5/552a (last visited Nov. 18, 2019). ↩

39. Paul M. Schwartz and Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 Geo. L. J. 115, 2017. ↩

40. *See* https://www.ftc.gov/policy/cooperation-agreements (last visited Apr. 1, 2020). ↩

41. Cal. Civ. Proc. Code § 1798.100 ↩

42. Business-to-Consumers. ↩

43. Business-to-Business. ↩

44. Consumers-to-Consumers. ↩
45. Leopoldo Angrisani, Pasquale Arpaia, Nicola Moccaldi, Antonio Esposito, *Wearable Augmented Reality and Brain Computer Interface to Improve Human-Robot Interactions in Smart Industry: A Feasibility Study for SSVEP Signals*, 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), (2018). ↩
46. Cf. Lee Lovevinger, *An Introduction to Legal Logic*, Indiana L. J., 27, 4 (1952). ↩
47. Norberto Bobbio, *Ibid.* ↩
48. *Id.* ↩
49. In opposition to the Realism doctrine that is more common in the America Common Law system, as it is based on the real meaning of the norm because it looks at the Law as it really is and not as it should be (precedent-based systems rely much more on sociology as the case-law is the direct expression of society, rather than the imposed law, as in Civil Law system. The Realism doctrine finds in Oliver Wendell Holmes its father and in Roscoe Pound its most prestigious theorists. ↩
50. Gabriele Lolli, *Logica e ragionamento giuridico*, at http://homepage.sns.it/lolli/articoli/giuridico.pdf (last visited Nov. 18, 2019). ↩
51. "ITIF Technology Explainer: What Is Quantum Computing?" Available at: https://itif.org/publications/2018/09/20/itif-technology-explainer-what-quantum-computing (last visited Dec. 17, 2019). ↩
52. Neil MacCormick, Rhetoric and The Rule of Law: A Theory of Legal Reasoning, Oxford (2005). ↩
53. Cf. James Boyd White, "Law as Rhetoric, Rhetoric as Law: The Arts of Cultural and Communal Life," The University of Chicago L. Rev, 52, 3, 684-702 (1985). ↩
54. Chaïm Perelman, Lucie Olbrechts-Tyteca, Traité de l'argumentation. La nouvelle rhétorique (1958), Université de Bruxelles, (2008). ↩
55. Other classical legal rhetorical figures are the "*commoratio*" (amplification), "*expolitio*" (dilatation), "*dubitatio*" (comparison), "*correctio*" (clarification), and "*ipotiposi*" (conceptualization). ↩
56. See The Association for Computational Linguistics, *What is Computational Linguistics*, (2005), at http://www.aclweb.org/archive/misc/what.html (last visited Nov. 18, 2019). ↩
57. Alex Pentland, *Social Physics*, Università Bocconi ed. (2015). ↩
58. GDPR Article 4 (2). ↩

59. GDPR Article 2. ↩
60. Ann Cavoukian, *Privacy by Design. The 7 foundation principles*, (2009), at https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf (last visited Nov. 25, 2019). ↩
61. FTC, Report on Protecting Consumer Privacy in an Era of rapid change, (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (last visited Nov. 25, 2019). ↩
62. Article 25. Cf. also Recitals 75 and 78. ↩
63. *Id.* ↩
64. G.W. van Blarkom, J.J. Borking, J.G.E. Olk, *Handbook of Privacy and Privacy-Enhancing Technologies. (The Case of Intelligent Software Agents)*, (2003), http://www.andrewpatrick.ca/pisa/handbook/handbook.html (last visited Nov. 25, 2019). ↩
65. Enigma, https://blog.enigma.co/welcome-to-enigma-start-here-e65c8c9125ef (last visited Nov. 25, 2019). ↩
66. OpenPDS, https://openpds.media.mit.edu/#architecture (last visited Nov. 25, 2019). ↩
67. *Id.* ↩
68. Thomas Hardjono, *A Federated Authorization Framework for Distributed Personal Data & Digital Identity*, ArXiv, abs/1906.03552 (2019). ↩
69. *See* e.g., User Managed Access Work Group, available at: https://kantarainitiative.org/groups/user-managed-access-work-group/. ↩
70. For legal phenomenon, I mean the set of subjects, legal acts, legal facts, legal effects and implications that compose a complicated situation, such as a trial. ↩
71. GDPR Article 13 ↩
72. Consent, legitimate interest, necessary contract and so on. ↩
73. Cf. Recitals 32 and 33. ↩
74. S.C. Kleene, *Representation of Events in Nerve Nets and Finite Automata*, Annals of Mathematics Studies 34, Princeton University Press, 3–41, (1956). ↩

75. Essentially, it works on the XOR logical operator, in which a specific neuron mediates the information between two other nodes and frame it in a sense or another. To oversimplify it, it works in a syllogistic way to connect two different information. ↩
76. Image source: https://www.kdnuggets.com/2017/12/deep-learning-made-easy-deep-cognition.html (last visited Nov. 18, 2019). ↩
77. Any approach to problem solving that employs a practical method not guaranteed to be optimal or rational, but which is however sufficient for reaching a rapid short-term goal. In AI systems it is adopted while searching a solution by exploiting some function that is coded into the system by the programmer or by adjusting the weight of branches based on how likely each branch is to lead to a goal node. Cf. Pearl, Judea, **Heuristics: Intelligent Search Strategies for Computer Problem Solving.** New York, Addison-Wesley, vii, (1983). ↩
78. Cf. Anna Trosborg, *Statutes and contracts: An analysis of legal speech acts in the English language of the law*, **Journal of Pragmatics** 23, 31-53, (1995). ↩
79. Image source: https://singularityhub.com/2019/03/17/finally-proof-that-quantum-computing-can-boost-machine-learning/ (last accessed Dec. 17, 2019) ↩
80. Article 832 of the Italian Civil Code, which describes the right of property and is titled "content of the right" (in book III "about property"; Title II "about property"; Chapter I "general dispositions"). [freely translated by the author]. ↩
81. E.g. the right to life and the right of self-determination. ↩
82. Ergo, at https://docs.accordproject.org/docs/ergo.html (last visited Nov. 18, 2019). ↩
83. As above. ↩
84. Cf. Harry Surden, *Computable Contracts*, UC Davis Law Review, 46, 629, (2012). ↩
85. Constitutional law, Ordinary law, State/Regional/Department law, and Local law. ↩
86. i.e. those resolvable with the approaches described in §2 (hierarchy, chronology, speciality). ↩
87. GDPR Articles 1 and 2. ↩
88. Constitutional law, Penal law, Private law and so on. ↩
89. Under or over a certain amount. ↩
90. Norberto Bobbio, *Ibid.* ↩

91. N. Bobbio, *Id.* ↩
92. N. Bobbio, *Id.* ↩
93. Peter Goodrich, **Legal Discourse: Studies in Linguistics, Rhetoric and Legal Analysis**, MacMillan Press, London (1990). ↩
94. e.g. the payment of debt deals with the discipline of obligations and both with the regime of Contract Law. ↩
95. such as consumer, employee, contract party and so on. ↩
96. It can be a right, an interest, a category of individuals, a situation, a material good and so on. ↩
97. I.e. the metaphorical reference to the set of people that drafted and approved the law, as the Parliament. ↩
98. Outside the borders of the systematic analysis. ↩
99. Ryan Calo, *ibid.* ↩
100. Cf. Grete Hermann, Dirk Lumma, "The Foundations of Quantum Mechanics in the Philosophy of Nature," The Harvard Review of Philosophy 7, 1, 35-44, (1999). ↩
101. See Arno Bohm, Quantum Mechanics: Foundations and Applications, 3rd ed., Springer (1993). ↩
102. Cf. Graziano Cavallini, La Costruzione probabilistica della realtà. Dalla Fisica Quantistica alla Psicologia della Conoscenza, Aracne (2018). ↩
103. R. George Wright, *Should the Law Reflect the World: Lessons for Legal Theory from Quantum Mechanics*, **18 Fla. St. U. L. Rev.** 855 (1991). ↩
104. Lawrence H. Tribe, *The curvature of constitutional space: What lawyers can learn from modern physics*, **Harvard L. Rev.** 103, 1, (1989); Amar Dhall, *On the Philosophy and Legal Theory of Human Rights in Light of Quantum Holism*, **World Futures**, 66:1, 1-25, (2010). ↩
105. V. I. Yukalov and D. Sornette, *Quantum decision theory as quantum theory of measurement*, **PHYSICS LETTERS A**, 372, 46, 6867-6871 (2008). ↩
106. See also Kristan Camilleri, Heisenberg and the Interpretation of Quantum Mechanics, Cambridge University Press, (2011); . Cf. R. Calo, id. About the concept of indeterminacy. ↩

107. Bart Verheij, *To Catch a Thief With and Without Number: Arguments, Scenarios and Probabilities in Evidential Reasoning*, **13 Law, Probability and Risk** 307-325 (2014). ↩

108. Lawrence H. Tribe, *ibid.* ↩

109. Norberto Bobbio, *ibid.* ↩

110. i.e. individuals: meaning non-divisible, exactly like "a-tom". ↩

111. Acts and facts, in order to be 'legal' must hold legal repercussions. Not every human action or fact is legal, as not all of them entails legal effects or consequences. ↩

112. Non-determinable a priori. ↩

113. Jerome R. Busemeyer, Peter D. Bruza**, Quantum Models of Cognition and Decision**, Cambridge University Press (2012). ↩

114. N. J. Nilsson, *Probabilistic logic*, **Artificial Intelligence** 28, 1, 71-87, (1986), among many. ↩

115. Pang Qi, Wang Haib, Xu Zeshui, *Probabilistic linguistic term sets in multi-attribute group decision making*, **Information Sciences**, 369, 128-143 (2016). ↩

116. Ross D. Shachter, Mark A.Peot, *Decision Making Using Probabilistic Inference Methods*, Uncertainty in Artificial Intelligence, Proceedings of the Eighth Conference, July 17–19, 1992, Eighth Conference on Uncertainty in Artificial Intelligence, Stanford University, 276-283 (1992). ↩