NEW TECHNOLOGIES AND LAW: GLOBAL INSIGHTS ON THE LEGAL IMPACTS OF TECHNOLOGY, LAW AS META-TECHNOLOGY AND TECHNO REGULATION

Ugo Pagallo[1]
Emre Bayamlıoğlu[2]
Colette Cuijpers[3]
Massimo Durante[4]
Marcelo Padua Lima[5]
Eduardo Magrani[6]
Mônica Steffen Guise Rosina[7]
Sunita Tripathy[8]
Rivka Weill[9]

Introduction

The starting point of our analysis on law and technology has to do with a basic fact: whereas, over the past centuries, human societies have used information and communication technology ("ICT"), but have been mainly dependent on technologies that revolve around energy and basic resources, today's societies are increasingly dependent on ICT and moreover, on information as a vital resource. The processing of well-formed and meaningful data is not only reshaping essential functions of current societies, such as governmental services, transportation and communication systems, business processes, or energy production and distribution networks. What is more, the information revolution is affecting our understanding about the world and about ourselves.

By insisting on the legal impact of the information revolution, it does not follow, however, that the law cannot regulate the process of technological innovation. On the contrary, the law can conveniently be understood as a technique that regulates other techniques and hence, as a meta-technology which competes with other

[1] Full Professor in Philosophy of Law - Faculty of Law, University of Turin, Italy.
[2] Assistant Professor - Law School, Koç University, Turkey.
[3] Director of Tilburg Institute for Law, Technology and Society (TILT) and Associate Professor - Tilburg Law School, The Netherlands.
[4] Assistant Professor in Philosophy of Law - Department of Law, University of Turin, Italy.
[5] Lawyer at *Cascione, Pulino, Boulos e Santos Advogados* and Researcher – Research Group on Law and Innovation at FGV Law School in São Paulo, Brazil.
[6] Assistant Professor and Researcher - Center for Technology and Society (CTS) at FGV DIREITO RIO, Brazil.
[7] Coordinator - Research Group on Law and Innovation and Full Professor - FGV Law School in São Paulo, Brazil.
[8] Assistant Professor and Assistant Director, Center for Intellectual Property & Technology Law, Jindal Global Law School, India.
[9] Associate Professor (tenured) - Radzyner School of Law, Israel.

modalities of regulation, such as the forces of the market or of social norms. In addition, the traditional hard tools of the law, such as statutes and codes supported by the threat of physical sanctions, have increasingly been complemented with more sophisticated forms of enforcement via the mechanisms of design, codes, and architecture.

This is the bread and butter of work on the regulatory aspects of technology in such fields as universal usability, informed consent, crime control, social justice, or design-based instruments for implementing social policies. From the viewpoint of the law as a meta-technology that competes with other forms of regulation, we thus assume a bidirectional tension, or interplay, between law and technology. Instead of a one-way movement of social evolution from technology to law, a key component of the legal challenges in an information society concerns the other way around, that is, how the regulatory tools of technology can be exploited by embedding normative constraints into the design of spaces (environmental design), or of objects (product design), or of messages (communication design), so as to comply with the rules of current legal frameworks.

On this basis, three different levels of analysis follow as a result, namely: (i) the legal impact of technology; (ii) the law conceived as a meta-technology; and, (iii) the field of techno-regulation, or legal regulation by design. More particularly:

(i) The legal impact of technology suggests that focus should be on how the current information revolution is affecting the tenets of the law. In addition to transforming the approach of experts to legal information, e.g. the development of fields such as AI and the law, technology has brought on new types of lawsuits, or modified existing ones. Consider new offences such as computer crimes (e.g. identity theft) that would be unconceivable once deprived of the technology upon which they depend. In accordance with the clause of criminal immunity summed up, in continental Europe, with the formula of the principle of legality, i.e. "no crime, nor punishment without a criminal law" (*nullum crimen nulla poena sine lege*), this is why international lawmakers decided to intervene with the Budapest Convention on cybercrime in November 2001. Moreover, reflect on traditional rights such as copyright and privacy, both turned into a matter of access to, and control and protection over, information in digital environments. By examining the legal challenges of technology, we thus have to specify those concepts and principles of legal reasoning that are at stake. Then can we begin to determine whether the information revolution: (a) affects such concepts and principles; (b) creates new principles and concepts; or, (c) does not concern them at all, the latter being the view of traditional legal scholars.

(ii) The law conceived as a meta-technology has to do with the old, Kelsenian account of the law as a social technique of a coercive order enforced through the menace of physical sanctions: "if A, then B." To be sure, law can be considered as a form of meta-technology without buying any of Kelsen's ontological commitments. Rather, we should pay attention to the impact of technology on the formalisms of the law, much as how legal systems deal with the process of

technological innovation, through such a complex network of concepts, as agency, accountability, liability, burdens of proofs, clauses of immunity, or unjust damages. In this latter case, the aim of the law to govern the field of technological innovation comprises several different approaches. Some, as Bert-Jaap Koops (2006), distinguish four main legislative purposes, such as: (a) the achievement of particular effects; (b) functional equivalence between online and offline activities; (c) non-discrimination between technologies with equivalent effects; and, (d) future-proofing of the law that should neither hinder the advance of technology, nor require over-frequent revision to tackle such a progress. Others, as Chris Reed (2012), propose to differentiate between (a) technological indifference, i.e. legal regulations which apply in identical ways, whatever the technology, such as the right to authorize communication of a work to the public in the field of copyright law; (b) implementation neutrality, according to which regulations are by definition specific to that technology and yet, they do not favour one or more of its possible implementations, e.g. the signature of e-documents; and, (c) potential neutrality of the law that sets up a particular attribute of a technology, although lawmakers can draft the legal requirement in such a way that even non-compliant implementations can be modified to become compliant. Vice versa, technology can be designed to leave no other options, being way more coercive then law. No matter how strict a legal rule and how fierce the sanction on disobedience; a rule leaves room to behave disaccording. If technology leaves no other option, the law as meta-technology can function as counterweight, possibly leading to conflicts between the two modalities of regulation. In this perspective, the law as meta-technology is the mechanism to limit the invasiveness of techno-regulation.

(iii) The field of techno-regulation, or legal regulation by design, concerns how current advancements of technology have obliged legislators and policymakers to forge more sophisticated ways to think about legal enforcement. Although some of these architectural measures are not necessarily digital, e.g. the installation of speed bumps in roads as a means to reduce the velocity of cars, the new scenarios of the information revolution have suggested national and international lawmakers complementing the traditional hard tools of the law through the mechanisms of design, codes, and IT architectures. Many impasses of today's legal and political systems can indeed be tackled, by embedding normative constraints and constitutional safeguards into ICTs. Whereas, in their work on *The Design with Intent Method* (2010), Lockton, Harrison and Stanton describe 101 ways in which products can influence the behaviour of their users, suffice it to dwell here on three different aims that design may have: (a) to encourage the change of social behaviour through incentives based on trust (e.g. reputation mechanisms), trade (e.g. services in return), etc.; (b) to decrease the impact of harm-generating behaviour through security measures, user-friendly interfaces, default settings, and the like; and, (c) to prevent harm-generating behaviour from occurring via the use of self-enforcing technologies. The latter appears the most critical aim of design, since people's behaviour would unilaterally be determined on the basis of technology, rather than by choices of the relevant political institutions and moreover, the normative side of the law would be transferred

from the traditional "ought to" of legal systems to what actually is determined by technical instructions. Leaving aside China's "Great Firewall" and the systems of filters and re-routers, detours and dead-ends, which aim to keep internet users on the state-approved online path, it is noteworthy that the repressive side of this design policy has shown up in Western democracies as well (Pagallo 2015). Two challenges to the rule of law are particularly striking. On the one hand, the use of allegedly perfect self-enforcing technologies raises serious threats of paternalism and, even, of authoritarianism, because such techniques as DRMs, automatic versions of the principle of privacy by design, three-strikes approaches to copyright enforcement, or systems of filters in order to control the flow of information on the internet, end up with the modelling of individual conduct. On the other hand, the aim of both lawmakers and private companies to increasingly tackle the challenges of the information era through the means of design, code, and IT architectures, that is, by embedding legal safeguards into information technology, often leads to the illegitimate condition where states claim to regulate unilaterally extraterritorial conduct by imposing norms on individuals who have no say in the decisions affecting them.

In accordance with this tripartite differentiation of law and technology, the intent of the paper is to further our understanding of the interplay between the legal impact of today's information revolution and the regulatory aims of the law, in light of some relevant practical cases for analysis. These cases suggest that we should draw attention to whether, or to what extent, technology is impacting basic tenets, principles, or concepts of the law and, vice versa, how the law intends to govern such fields.

Should we endorse the criterion of functional equivalence between off-line and ICT-driven activities, or rather the principle of implementation neutrality vis-à-vis that of non-discrimination? Are there further approaches at hand? Is the choice of this meta-technological policy mostly context-dependent, or there is room for some kind of generalization? Should the legal regulation of technology be conceived as an end in itself or should focus be on the social and economical outputs of people adopting a certain technology? How about the alternative between law as meta-technology and techno-regulation? Does the latter inexorably affect the corollaries of the rule of law?

In an attempt to answer some of these questions, the paper is divided into 4 chapters, based on the systematization we have proposed above: (i) legal impacts of technology; (ii) law as meta-technology; (iii) techno-regulation; and (iv) a final case study that analyses technology as a cause of the problem, but also as an enabler and enforcer of the solution. Each chapter first dwells upon a more theoretical reflection of its domain and then moves into specific cases that can shed extra light on the interplay between law and technology.

I. LEGAL IMPACTS OF TECHNOLOGY

A. Theoretical Approach: online trust in reputation systems

Cyberspace increasingly supports a variety of agents, from human to artificial agents. When interacting in multi-agent systems, we rely more and more on the human/machine interface for communication, information, transactions, business, without being always able to ascertain whether we interact with human or with artificial agents. Furthermore, multi-agent systems often require not only reliance on the machine interface protocols but, first and foremost, trust in someone else's behavior for the success of operations, negotiations and relations based on computer-mediated interaction or coordination between individuals or groups (Taddeo 2009 and 2010). As argued elsewhere (Durante 2008 and 2010), our normative understanding of possibly trustworthy interactions is field-dependent: i.e. it depends on the context it occurs in, and varies according to the nature of the agents we interact with.

Thus, the issue of trust-building in web technologies-based environments depends on what is the type of normativity in the context of interaction and on what the nature is of the interacting agents: human/human (H>H); human/agents (H>A); agents/human (A>H); agents/agents (A>A) (Grodzinsky, Miller & Wolf 2010). Let us concentrate our attention on the normativity of context as the general theoretical and practical framework in which trust is related to security, which also raises the issue of technological and legal normativity.

In this respect, we think that building trust is not only a matter of assuring technological or legal security by means of rules, constraints, protocols, architectures, and guaranties. Technological or legal security is particularly necessary in the context of online commercial transactions, privacy issues, or legal contracts, but it does not suffice to assure that trustworthy interactions are displayed in the context of social cooperation. In fact, this is to be based on the agent's behavior, on its willingness to cooperate with us that is never fully predictable nor can it be automatically subject to control or implementation. On the contrary, it is mainly concerned with social and cognitive dispositions towards other agents that are to be envisaged within the framework of a model of networked trust.

Let us sum up what we have said so far by stating three different normative principles that govern the process of how we try to secure that a particular goal is obtained by means of someone else's behavior:

A) A *principle of compensation* concerning legal security.
   Legal security is required as long as agents' interaction can be based on a rule of compensation: in such cases, the agents' desired goal can be efficiently substituted by a second-best goal. In this regard, law is a system of expectations and of rules compensations, which apply when expectations are

frustrated. In other words, one interacting party is expected to provide the other with compensation in case of defection. From a cognitive standpoint, the legal system is based on expectations as well as a trust system but it assures *compensation over trust*, firstly[10]. For this reason, it is actually said to be based on parties' mutual distrust (Chiodi 2000; Scillitani 2007; Resta 2009), even though distrust is ultimately based on parties' trust in the effectiveness of a third authority (e.g. a judge), called upon to apply the rules of compensation (Durante 2008);

B) A *principle of prevention* concerning technological security.
Technological security is required as long as interacting parties believe that agent's expected behavior does not suffice by itself to secure the desired goal, nor are they satisfied with a second-best goal assured by means of compensation. One party intends to prevent the other from not fulfilling the expected task: this system assures *prevention over trust*. It is actually based on the parties' common distrust, since all parties share distrust in the effectiveness of a third authority called upon to apply the rules of compensation. In this respect, trust is displaced from parties or authorities and is placed on technological devices (which are often suggestively called "trusted systems"). However important, prevention should not always prevail over trust: "My own preference would be for a progressive social vision of cyberspace that preserves the degrees of freedom that trust needs. At the same time, we ought to develop technologies of security that might make possible pockets of high security for the kinds of transactions that call for it, without making that the dominant norm throughout" (Nissenbaum 2004, 179).

C) A *principle of cooperation* concerning trust.
Trust is required as long as agents' interaction cannot be solely based either on rules of compensation nor on trusted systems of prevention. One interacting party cannot (or prefers not to) obtain a desired goal if not relying on the other party's willingness and ability to fulfill the delegated task, that is, taking the risk to entrust someone else. This system assures *trust over security*. It is based upon a mutual relation of common trust: "The key behavior of the agents to enable them to form cooperative group is that they shift their probability of cooperation or defection based on the expected behavior of the majority of its neighbors, i.e. if the majority of neighbors play defect then each agent will increase the probability that it defects, and the same for cooperation" (Ghanea-Hercock 2007). Furthermore, expected behaviors are reinforced by sharing common concerns for a goal: "Trust-based online cooperation proves to be reasonable whereas it is teleologically aimed to a

[10] Some scholars talk of legal normativity in terms of "recourse" instead of compensation but the idea is roughly the same. See for instance J.-G. Hurwitz, 2013, 1597-1598: "The law offers a simple alternative to trust: remedies. In contrast to trust-based institutions' premise of reliance *without* recourse, legal institutions stand on the promise of reliance *with* recourse. Where parties are unable to rely on one another due to the lack of trust, the law steps in as an external institution to enforce parties' expectations, thereby allowing them to rely on one another without jeopardizing their security".

> specific goal of common concern grown out of a communication process drawing the framework within which it is reasonable to expect a determined behaviour from another agent" (Durante 2008).

One example can explain how these principles can apply according to a different *level of abstraction* (Floridi 2008). Let us imagine the relation between a producer and a musical band. Firstly, the producer is interested in the fact that the musical band will perform, during the year, a certain number of concerts. She will make the band sign a contract, in order to provide herself with compensation, in case of defection (*principle of compensation*). Secondly, the producer is interested in the fact that the band will perform a concert, even if the band is not in a fit condition for playing. She will make the band perform the concert by means of playback, in order to prevent them from not fulfilling their expected task (*principle of prevention*). Thirdly, both the producer and the band are interested in showing that the band is a great live performer: all of them need to trust each member of the musical band that they will be able to perform the common task (*principle of cooperation*). In such cases, each normative principle may apply according to the type of goal that is meant to obtain in the specific context at stake[11].

Whether "the Internet's early architecture was built on a foundation of trust" (Hurwitz 2013, 1580), the current and more stratified architecture of the Internet is built on the interplay between different normative principles (*law, technology and trust*), which may concur or compete with each other. The analysis based on levels of abstraction may allow us to disentangle such an interplay and shows us what principle applies in what context. This has changed the perception of trust-based online interaction as it concurs or compete with technological and legal normativity. Hurwitz has even suggested that we entered into a "post-trust Internet", where "the increasing complexity of the network – especially with the rise of active intermediation – and the transition away from a small community of users generally interested in the success of the internet and toward a large user base" have been the primary drivers of this change of paradigm. He also remarked that this change "is problematic because it is unclear what can replace trust – a willingness of users to rely on the Internet architecture without assurances that recourse is available should they be harmed – as a foundation for online interaction" (Hurwitz 2013, 1597). We believe that the evolution of the Internet architecture supports (and is characterised by) the interplay of diverse normative principles so that more and more online interactions and mechanisms can nowadays be fully and suitably appraised through the

[11] In relation to legal and technological, we may also say that diverse levels of abstraction or field dependency require a different perspective in the study of online trust insofar as the functioning of multi-agent systems demands cooperation: 1. from gained security to perceived security (i.e. security as it is perceived by agents disposing of incomplete information); 2. from control trust (i.e. trust based on control tools and mechanisms for assessing trustworthiness) to party trust (trust based on the dynamic interaction between a party, the trustor, and a counter party, the trustee); 3. from a model of probabilistic trust (based on rigid methods of statistical inferences) to a model of cognitive social trust (i.e. based on beliefs, expectations and concerns).

disentanglement of such normative interplay. Sometimes, online interactions or mechanisms are guided by (a) *only one normative principle*: in such cases, they are based either on law, technology or trust as normative principles guiding the way to secure a specific goal by means of online interactions or mechanisms. More often, online interactions or mechanisms are guided by (b) *the interplay of different normative principles*: this interplay can be characterised by different share and combination of law, technology and trust. In such cases, it is important to disentangle and appraise the role played by each normative principle (or some of them). It may also happen that online interactions or mechanisms that seem to be governed by only one normative principle (c) actually *make appeal to more than one of them*.

For instance, reputation mechanisms based on review or recommendation systems seem to appeal exclusively or mostly to trust (conceived both in relational and epistemic terms). People rely on someone else's review or recommendation to get information directing their mind to a specific choice because there is not, most of times, a legal or technological manner to have this information shared. Nonetheless, review or recommendation systems are also often characterised by the more or less apparent interplay with other normative principles. Let us illustrate this point by means of some examples.

"Shopping sites, such as Amazon, encourage consumers to create online reviews for products through product reviews. Such review systems enhance the value of Amazon and eBay as shopping destinations. However, Amazon takes it one step further by allowing other consumers to rate the reviews, creating reputation systems for reviewers. Those reviewers with the highest ratings are given greater prominence" (Matta and Frost 2011, 1). Rating the reviews is a reputation tool that impinges, at least in part, both on technological and legal normative attitudes. Rating the reviews is mirroring a control system based on cycle of information feedbacks (Durante 2010, 355; Ghanea-Hercock 2007), which requires, on the technological side, design choices (in order to rate the reviews and track the trail of reviewers' behaviours, thus profiling the reviewers by means of their behavioral patterns), and, on the legal side, the normative attitude at either approving or reproving reviewers' behaviours.

Yannis Bakos and Chrysanthos Dellarocas (2011, 1) argue, from an economic standpoint, that "the popular view of reputation as an efficient and relatively costless way to induce seller effort under all circumstances is incorrect; reputation is less efficient than litigation in inducing any given level of effort. Thus reputation improves efficiency only in settings where the high costs of litigation, insufficient damage levels or low court accuracy induce sub-optimal effort or cause market failure. When adverse selection is important, reputation helps reveal the true types of market participants, which may offset its higher cost of inducing effort. Finally, adding reputation to existing litigation mechanisms increases seller effort and may require adjusting damage awards to avoid inducing over-effort". This study shows that the interplay between reputation models, based on trust, and litigation-like mechanisms for dispute resolution, based on law, is much deeper than expected and is consistent with both competition and concurrence between the two mechanisms of inducing seller effort.

Matthias Wibral compares two experimental markets, where buyers can rate sellers after each transaction. The only difference is that "sellers in one market can change their identity (*change treatment*), i.e., erase their rating profile and start over as new players, while in the other market this is not possible (*no change treatment*)" (Wibral 2014, 1). His study suggests that "buyers trust and seller trustworthiness are significantly lower when sellers can change their identities. Trust is especially lower for new sellers. However, the reputation system in the change treatment maintains trustworthiness at a level that is high enough to make investing profitable for the buyers. The evidence is at least suggestive that trustworthiness is also higher than in complete absence of a reputation system" (Wibral 2014, 2). Regulation on online identity construction, privacy norms and settings at large and more recently all legal provisions related to the right to be forgotten (on this topic see Pedro Letai's contribution in the paper) tend to delimit our capacity to have access to someone else's online reputation. Legal and social norms are crucial factors in shaping our capacity to have access to someone else's past. In so doing, they play a crucial role in the process of trust building through reputation systems.

Justin Hurwitz even claims that reputational models do not entirely reside on trust, since "these mechanisms (indeed, all mechanisms that rely on actors within a system to establish trust) are built upon the fundamental assumption that parties being relied upon to establish trust are independent from the party for whom trust is being established" (Hurwitz 2013, 1603). To put it differently, reputation models rely necessarily on the epistemic authority of a trusted third party (i.e., reviewers or reviewers of reviewers) not directly involved in the trustful relation, as law does, for instance, when one makes appeal to a judge, or technology, for instance, through encryption, which resides on a trusted third party, called a certificate authority.

All these examples bring us back to our starting point. Online interactions or mechanisms in reputation systems are field-, agent-type and goal-dependent: namely, they depend on the context they occur in, and they vary according to the nature of interacting agents and the type of goal that is meant to obtain in the specific context at stake. Furthermore, this context is mostly structured by (and can be thus accounted for in terms of) the interplay between three normative principles: i.e., legal compensation; technological prevention; and trustful cooperation. In conclusion, reputation systems vividly show how articulated and stratified such a regulative interplay between normative principles might be, contrary to their representation as mechanisms solely based on just one normative principle (*e.g.* online trustful relations).

B. Cases related to the domain: Amazon India and Encrypted Currencies

Amazon India

Cases of illegal online pharmacies,[12] grey and black marketing[13] through e-commerce channels are on the rise worldwide as also in India (Biswarupt et. al, 2014 and Sarkar, 2015). The fundamental basis for e-commerce as such, is that it is entirely consumer-driven and holds consumer welfare qualified by convenience and quality-control dear to its success. Digital aggregators have an intermediary yet crucial role in the online marketplace as they are the ones who bring the buyers and vendors together under one space, generate awareness and enable consumer preference determination. The consumer testimonials, feedback and ratings lead to the upgrade of goods and services within sectors; thereby fostering competition between vendors which influences pricing of such goods and services. Digital platforms are not merely spaces which enable payment gateways for the customer but, as noted by OECD, may provide a range of often bundled services such as 'fixing prices, transaction processing and co-ordination, quality guarantees, monitoring, as well as, in some cases, stock management.' (OECD, 2010). Consequentially, digital aggregators can be identified not only as online 'market creators' but also as ones who maintain the market so created.

The consumer's decision to purchase any good or service online is often based on his/her confidence in the digital aggregator's brand name.[14] Therefore when a consumer receives a delayed delivery or a fake product, or when the brand does not honour the warranty for such deficiency in service, concerns related to accountability arise.

The Indian Courts are yet to determine the liability, if any, of a digital aggregator operating via a third-party marketplace model. The Division Bench of the Delhi High Court has in the matter of World Wrestling Entertainment, Inc v. M/s Reshma Collection (decided on October 15, 2014) conclusively held that "jurisdiction in e-commerce cases involving trademark and copyright disputes would be determined by the **buyer's place of residence**"[15] thereby reiterating that the

---

[12] *See* more at Indian Express, "FIR against Snapdeal CEO Kunal Bahl, 5 firms for selling drugs online." (Date May 02, 2015) Available: http://indianexpress.com/article/business/business-others/fir-against-snapdeal-ceo-kunal-bahl-5-firmsfir-for-selling-drugs-online/ (accessed on June 15, 2015).

[13] Consumer feedback regarding fake products on Amazon India, Available: http://www.amazon.in/product-reviews/B00MMKAVR8 (accessed on June 14, 2015); "Counterfeit Xiaomi Power Bank being sold on Snapdeal", available online: http://techivian.com/counterfeit-xiaomi-powerbank-sold-snapdeal/ (accessed on June 14, 2015). Also see, customer reviews regarding fake products being sold online: http://en.miui.com/thread-76172-1-1.html (accessed on June 14, 2015).

[14] Conclusively, vendors also choose to list themselves with such digital aggregators, rather than sell through their own portals because of the robust online infrastructure in the nature of the e-commerce website made available by Amazon like digital aggregators and also because of the tremendous reputation enjoyed by such brand.

[15] See, judgement here: http://indiankanoon.org/doc/71641182/ (accessed on June 12, 2015); The Division Bench relied on the judicial reasoning in the landmark case of Bhagwandas Goverdhandas Kedia v. Girdharilal Parshottamdas & Co., AIR 1996 SC 543, and reiterated that while the general rule of acceptance of any contract being that, the contract is complete when the offeror receives intimation that the offeree has accepted his offer; the exception to

convenience of the end-user is the most important goal of any service industry.[16]

For the purpose of addressing the interaction between law and technology in order to ensure that the digital aggregators who are drivers of e-commerce be encouraged to take a proactive role rather than a defensive role in containing the illegal activities of its vendors and participate in devising robust industry regulatory mechanisms that minimize aberrations leading to consumer exploitation on the part of such deviant vendors, the marketplace model of one such Indianized[17] digital aggregator, which enables third party vendors to reach consumers, namely Amazon India is discussed herein as a practical case study.

In the year 2000, Amazon broadened its focus from being a purely product based entity namely an online book-seller to being a platform based entity offering a

---

this general rule is when the contracts are negotiated by postal communication or telegrams, the contract would be said to be complete when the acceptance of the offeree is put into a course of transmission by him/her by posting a letter or dispatching a telegram. In the Bhagwandas case the Supreme Court had held that offer and acceptance via instantaneous communication such as telephonic conversation would not attract the exception to the general rule of contract. See also, Devika Agarwal, "Jurisdiction in E-Commerce IP Disputes" (October 18, 2014) available online: http://spicyip.com/2014/10/jurisdiction-in-e-commerce-ip-disputes.html (accessed on June 02, 2015). Further the Court observed that the catalogued list of goods and services on an e-commerce website constitute an 'invitation to offer' while the consumer's order to purchase any goods and services so displayed constitute 'an offer' to buy. When a consumer who is based in Delhi, successfully makes a purchase through confirmed e-payment that is when the offer to buy is said to have been accepted by the online vendor. As this transaction takes place instantaneously, the communication of acceptance by the online vendor is also said to be instantaneously communicated to the consumer through the internet at Delhi. Therefore, it is considered that the essential part of the vendor's business is being carried out at Delhi.

[16]Reliance was placed upon the Supreme Court's three-pronged test laid down in the matter of Dhodha House v. S. K Maingi (2006 (9) SCC 41) to determine the appropriate forum for litigants, and the interpretation of the expression '***carries on business'*** as entailed in Section 134 (2) of the Trade Marks Act, 1999 and Section 62 (2) of the Copyright Act, 1957 to mean that a person may not necessarily carry out the business by himself but may do so even through a servant or **an agent**. The conditions set out by the Court include: (i) The agent must be a special agent who attends exclusively to the business of the principal and carries it on in the name of the principal and not as a general agent who does business for anyone that pays him; (ii) The person acting as agent, must be an agent in the strict sense of the term and a manager of a Joint Hindu Family cannot be regarded as an agent within the meaning of this condition; and (iii) To constitute carrying on business at a certain place, the essential part of the business must be performed at that place. As the Appellant did not have any 'agent' in Delhi, the Hon'ble Division Bench went ahead to examine if the third condition was being fulfilled in the instant case, i.e., whether an essential part of the Appellant/Plaintiff's business was being performed at Delhi. To determine this, the Court invariably dealt with the question of where a contract is concluded when the transaction takes place over the internet.

[17]Amazon.com, Inc. is a NASDAQ-listed American electronic commerce company with headquarters in Seattle, Washington USA and has operationalized an Indian Franchise named Amazon India. According to Michael De Kare-Silver (2014, 101): "Amazon has 175 million active accounts worldwide and that has led to $75 billion in global revenues".

marketplace for the end-user as well as complementor service oriented business (Balwin and Woodard, 2009). This transition in the business model marked a transformation of its organizational identity leading to accounting of newer metrics for measuring the success of such business model (Altman and Tripsas, 2015)[18]. The indicators included the number of vendor subscriptions as also the total number of transactions between such vendors and the consumers which consequentially materializes into royalty payments.

Advertising itself as the "Earth's most consumer-centric company"[19] Amazon complimented its marketplace with a branded guarantee program promising a full refund to the consumer in the event of receiving defective products from vendors listed with Amazon's marketplace. With market analysts forecasting a compound growth rate of the Indian market to reach $8.8 billion in 2016, which would be faster than any other country in the Asia-Pacific region (Widger et. al., 2012), Amazon found the time ripe to launch Amazon.in[20] with a third-party marketplace model in June 2013.[21] With the backing of its long-term stock investors, Amazon has the opportunity to capture the market share of e-commerce in India.

There are two ways that a vendor can be part of the Amazon.in catalogue: (a) vendors list-pack-ship and deliver directly to the consumer. The prices of goods and services are determined solely by the vendors. The absence of any direct interface between the retail buyer and the online portal leads to a situation where the digital aggregator will have no opportunity to verify the authenticity of the goods shipped by the vendors. In such case, if a consumer complaint regarding delivery of a faulty good is received, the vendor who is bound by User agreement is to refund full value of the good or replace the good with a genuine one instead. However, if the vendor dishonours warranties, it can at best be de-listed if and when Amazon India takes cognizance of such deficiency in service and decides to clean its platform. (b) vendors sign up to a service, which is advertised as the "Fulfillment by Amazon" Program (FBA).[22] This service assures the consumer that products are being warehoused and delivered by Amazon India. Essentially, Amazon India relies on the quality check mechanisms in place at their respective Fulfillment Centers to be confident about the genuineness of the goods and services being sold to the end-user. In case a fake good is delivered to the end-user in spite of such quality checks, the warranty is to be honored and the complained fake product is to be replaced with a genuine one. Amazon India also offers customers A-to-Z guarantee[23] for products to be delivered

---

[18] See also, S. Albert and D.A Whetten, (1985) Organizational Identity, *Research in Organisational Behaviour* 7, 263-295.

[19] Amazon Inc., (2015), [Mission or Vision Statement] available online : http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-faq#14296 (accessed on June 12, 2015)

[20] See http://www.amazon.in/ (accessed on June 02, 2015).

[21] "Amazon's perfect timing for India" (July 02, 2013) available online at http://forbesindia.com/article/big-bet/amazons-perfect-timing-for-india/35517/1 (accessed on June 02, 2015).

[22] Fulfillment-By-Amazon, Amazon Services, available online at: http://services.amazon.com/content/fulfillment-by-amazon.htm (accessed on June 14, 2015).

[23] Amazon's A-to-Z Guarantee Proetction available online at

in good-condition and in a timely manner. However it is to be noted that the A-to-Z guarantee does not assure against manufacturing defects in a product. Such responsibility is to be borne by the vendor.

The operational account related to the working of Amazon India clarifies that the goods and services listed in the catalogue of the e-commerce website are not owned by the digital aggregator.[24] The consumer protection law in India is silent about the responsibility of the digital aggregator as a self-regulator, in the e-commerce space. That leads us to gain an understanding of the legal status of a digital aggregator in Indian e-commerce law and its role in ensuring that a consumer's online trust in its branded digital marketplace is protected.

The definition of an 'intermediary' under the Information Technology (Amendment) Act, 2008 (hereinafter referred to as the 'IT Act')[25] clearly envisages online-market places created by digital aggregators such as Amazon India within its realm.[26] Section 79 of the IT Act provides immunity to Internet Service Providers (ISPs) in certain cases of internet wrongs committed through their networks provided they follow due diligence available in Information Technology (Intermediaries guidelines) Rules, 2011. The intermediary will not be liable "for any third party

---

http://www.amazon.com/gp/help/customer/display.html?nodeId=537868 (accessed on June 12, 2015).

[24] Though the commercial tax department of the State of Karnataka recently alleged that Amazon should be paying the sales tax for all the orders placed with it through its Fulfillment service, and claimed that Amazon owns the goods for all 'practical' purposes. However Amazon clarified that it is an intermediary and not the owner of the goods sold by the vendors. See, Riddhi Mukherjee, "E-commerce marketplaces are liable for VAT since they are Commission agents - Karnataka Govt" (October 21, 2014) available online http://www.medianama.com/2014/10/223-karnataka-govt-online-marketplace-vat/ (accessed on June 02, 2015). The Karnataka Value Added Tax Act, 2003 and the Karnataka Value Added Tax Rules, 2005 available online at : http://dpal.kar.nic.in/English%20Act.pdf; Also Amazon being a company functioning as a marketplace model is an entity which does not own inventory as it does not buy any goods but brings retail customers and vendors together; and is therefore not required to comply with the foreign direct investment (FDI) restriction in India. See, Business Standard, "Amazon to follow marketplace model" (June 2013) available online at http://www.business-standard.com/article/companies/amazon-to-follow-marketplace-model-113060500216_1.html (accessed on June 10, 2015). See also, S. Muralidharan, "is the marketplace model adopted by Flipkart, Amazon India violating FDI norms" (May 02, 2014) available online at : http://www.firstpost.com/business/corporate-business/is-the-marketplace-model-adopted-by-flipkart-amazon-india-violating-fdi-norms-1969779.html (accessed on June 10, 2015).

[25] The Information Technology (Amendment) Act ,2008 available online : http://deity.gov.in/sites/upload_files/dit/files/downloads/itact2000/it_amendment_act2008.pdf (accessed on June 14, 2015)

[26] The Information Technology (Amendment) Act, 2008 (hereinafter referred to as the 'IT Act') defines an intermediary as:

"[a]ny person who on behalf of another person receives stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, webhosting service providers, search engines, online payment sites, online auction sites, **online-market places** and cyber cafes."

information, data, or communication link made available or hosted by him, if the intermediary does not initiate the transmission, select the recipient or select or modify the information"[27] Intermediaries are to conduct cyber law due diligence which requires them to publish all terms and conditions as also maintain customer privilege by ensuring data privacy online.[28] Failure to respond and redress complaints within thirty-six hours of its filing is also a ground for legal action against Internet Service Providers in India.

Given that the digital aggregator's function of providing the platform for enabling vendor discovery by the consumer becomes the first trigger for any transactional interaction between the vendor and the consumer, the immunity prescribed under section 79 when interpreted literally cannot be extended to digital aggregators.

An enquiry into the quality control mechanism adopted by Amazon India by MediaNama, a reliable data journalism initiative[29] reveals that the digital aggregator claims no liability as to the genuineness of the vendor's product prior to shipment. Instead it takes *post-facto* measures such as periodically conducting random checks via mystery shopping on vendors that have received poor consumer feedback and delisting them upon verification thereon. This system is essentially to cleanse its platform off counterfeit and fake goods.[30] Other metrics to ensure consumer satisfaction include recording the details of the counterfeit complaints, measuring the size of the problem and having mechanisms in place to control the menace of entry of fake goods into the marketplace.

If consumer trust in the online marketplace is to be built and maintained, the cyber law due diligence rules ought to also include mandatory verification of the credibility and delivering capacity of vendors who are aggregated, solicited or invited to contract with consumers on the online marketplace offered by the digital aggregators. Therefore, a consumer protection regulator for defining the processes and accountability in the value chain as also overseeing the effective compliance of quality standards to meet consumer expectations is the effective way to build a robust regulatory framework.

This consumer regulator may also maintain an account of the vendor's criminal history that can be accessed by the digital aggregator to make an informed decision while contracting with its subscribers. Presently, for the aggregator to be held

---

[27] *Supra.*

[28] See, "3. Due Diligence to be observed by Intermediary" of Information Technology (Intermediaries Guidelines) Rules, 2011 available online at http://deity.gov.in/sites/upload_files/dit/files/GSR3_10511(1).pdf (accessed on June 14, 2015).

[29] MediaNama is the premier source of information and analysis on Digital and Telecom businesses in India, available online at http://www.medianama.com/about/ (accessed on June 14, 2015).

[30] "How Amazon India deals with fake products" (October 22, 2014) available online at http://www.medianama.com/2014/10/223-amazon-india-fake/ (accessed on June 14, 2015).

liable for the illegal acts of its agents, no prior agreement to the contrary must be in place between the vendors and the aggregator; Once a functional consumer regulator having techno-regulatory powers is in place, such contractual arrangements can be understood to be going against the letter and spirit of e-commerce regulations in India.

With increase in the instances of disregard of the 'duty of care' on the part of vendors listed with digital aggregators, there is a need for stronger consumer protection measures. Limited control over the vendors activities, cannot be accepted as a valid excuse by the digital aggregators such as Amazon anymore, should they be interested in customer retention as also enhance customer acquisition for profitable gains. The social policy mandate for consumer welfare for creation of a sustainable online environment for e-commerce, can be achievable when distinct responsibilities or guidelines including positive tenets of the principle of 'vicarious liability' qualify the legal status of a digital aggregator as an 'agent' for e-commerce and not purely an intermediary. In this sense, the State needs to elicit active participation of all concerned stakeholders, namely the digital aggregator that is the platform provider, the vendor of good faith, the consumer and the State itself to build a vibrant ecosystem for e-commerce in India.

Encrypted Currencies

Another practical case worth noting when it comes to the interplay between law and technology is that of encrypted currencies, as they provide a good example of the relevant impacts that new technologies can have over law. Up until recently, the monopoly of countries over currencies was consolidated and virtually unchallenged. As a result, law and regulation were created, shaped and developed in most countries under the paradigm that only a single currency (the State issued and controlled currency) would be accepted as medium of payment within the borders of each country. However, over the past years, new technologies have enabled the creation of digital private currencies, such as the encrypted currencies and, particularly, the Bitcoin. This recent development can potentially break the paradigm mentioned above and affect several areas of the law.

As capitalism evolved in the last centuries, countries have gained and consolidated a centralized control over currencies, adopting a single currency as legal tender in its respective territories. National currencies are an important element of sovereignty, being usually issued and controlled by the national government[31]. Monopoly over the national currency allows a country to implement a more effective monetary policy, permitting control over the money supply and its cost. This is

[31] For example, in Brazil the major shift towards having the national currency as legal tender took place in 1933, when Decree No. 23.501 was enacted. Under this Decree, national currency became legal tender for all payment stipulations in the country and payment stipulations in gold, in different currencies or which could restrict or deny the legal tender of national currency became null and void. For information about the government monopoly over currency in the United States, see GRINBERG, 2012 and GLADSTONE, 1997.

essential to foster economic growth and to control inflation rates. Therefore, such monopoly is strategic and extremely relevant to most countries worldwide (Verçosa, 2015).

In view of the above, most payment systems, civil laws, foreign exchange laws, tax laws, anti-money laundering and terrorism financing controls, among others, were designed and structured worldwide under the basic assumption that countries will have monopoly over their respective currencies. Notwithstanding the foregoing, private currencies have been gaining visibility recently, in particular with the development of new technologies, such as the internet, software and complex encryption methods. The internet has enabled creation and growth of electronic commerce, electronic payment systems and electronic currencies, while sophisticated software and encryption methods were essential to design private electronic currencies, secure online transactions and control the supply and ownership of such currencies.

Although there are several different private currencies available nowadays, this section of the paper will analyze the Bitcoin, which is probably the most popular private currency today. Bitcoin is a digital, intangible and decentralized currency, which is not issued or controlled by a particular government, legal entity or individual. It is also not backed or redeemable for gold, other currencies or any other commodities. Bitcoin's soundness is based mainly on encryption and the ongoing work of the developers. Transactions involving Bitcoins are public, but the identities of the parties are not disclosed[32]. So far, Bitcoin remains in a grey, unregulated area. Even though certain private currencies are prohibited in some countries[33], most countries allow Bitcoin[34].

The potential growth and widespread adoption of encrypted currencies, such as the Bitcoin, pose challenges to different areas of the law. These challenges vary from country to country, based on the existing legal and regulatory framework. The scope of this section is to discuss certain general aspects of the Bitcoin, which are likely to be relevant in most jurisdictions, and to comment on how such aspects may affect local laws and regulations.

The first issue to be addressed in most jurisdictions is how to define the

---

[32] Please refer to the European Central Bank report, "Virtual Currency Schemes", issued in October, 2012, for a detailed explanation on how Bitcoin works. Available at: <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Access on: 30 June, 2015.

[33] A good example of a prohibited currency is the Liberty Dollar, a private currency backed by precious metals, which was prohibited by the United States of America. For more details on the prohibition of the Liberty Dollar, see GRINBERG, 2012.

[34] Certain countries, such as China, Russia and Iceland, have, totally or partially, prohibited the use of Bitcoin. Please refer to the briefing on "Bitcoin – Market, Economics and Regulation", issued by the European Parliamentary Research Service, available at: < http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2014/140793/LDM_BRI(2014)140793_REV1_EN.pdf>. Access on: 16 June, 2015

Bitcoin. Although Bitcoin is usually referred to as a currency, there are many controversies as to whether it should really be considered as a currency or not. Currencies typically have three different functions: (i) medium of exchange; (ii) unit of value; and (iii) store of value (Yazbek, 2007). Bitcoin, however, is not a conventional national currency, has limited acceptance in the market, is not commonly used to price goods or services and has been remarkably volatile over the last years. As a result, it is possible to question whether Bitcoin should be considered a currency or something else. Some people, for instance, argue that Bitcoin is better defined as a security, since it is closer to an investment than a currency[35].

In most countries, the treatment applicable to currencies is drastically different from the treatment applicable to securities. Currencies are usually regulated by the central banks and monetary authorities, while securities are usually regulated by securities commissions. Central banks and monetary authorities tend to be concerned with the conduction of monetary policy, systemic risk and soundness of the banking system, while securities commissions tend to be concerned with the protection of investors and with the development of the local capital market. As a result, there may be relevant impacts to Bitcoin depending on how it is defined.

Assuming that Bitcoin is a currency, the next issue to be addressed is whether it is lawful in a country to use a foreign currency to make local payments. For instance, certain countries adopt laws establishing that the national currency is legal tender and that local payments using foreign currencies are unlawful. In these cases, the use of Bitcoin is unlawful and the future of this currency is seriously at risk (at least in that country).

Most restrictions on the use of foreign currencies in a country's territory, as the one mentioned above, are intimately related to that country's choice to have the means to implement an effective monetary policy, allowing a real control over the supply of money available in the market. This is an essential measure to control inflation levels. Therefore, to accept the use of Bitcoin within the country's territory may weaken the effectiveness of the monetary policy, potentially affecting control over inflation rates.

Even in situations where it is lawful to use Bitcoin for local payments, another important issue is whether the local financial institutions are allowed to deal with Bitcoin or not. China has recently prohibited local banks from dealing with Bitcoin, while individuals are allowed to deal with it[36]. By prohibiting financial institutions from dealing with Bitcoin, a country's regulator may be trying to protect the financial system from a new, relatively opaque and complex currency. However,

---

[35] The definition of Bitcoin as a security is a controversial matter in certain jurisdictions, like the United States of America. For a detailed analysis on the matter in that country, see GRINBERG, 2010.

[36] "China bars banks from Bitcoin transactions", available at: <http://www.reuters.com/article/2013/12/05/us-china-bitcoin-idUSBRE9B407L20131205>. Access on: 29 June 2015.

such measure tends to push Bitcoin to informality and may impair its development.

Another important issue, particularly for countries that adopt foreign exchange controls, is to determine if and how the existing controls will apply to Bitcoin. In the absence of specific regulation in this regard, it is likely that transactions with Bitcoin will be performed regardless of the existing controls or, even worst, with the specific intention to circumvent such controls.

This leads to another important issue associated with Bitcoin, which is how to prevent the use of this currency for illegal purposes. The grey area where Bitcoin currently lays raises several concerns in connection with the potential use of Bitcoin to purchase illegal content (drugs, stolen goods, weapons etc.), to bribe government officials, to carry out tax or currency evasion, to laundry money deriving from illicit activities (Hoffman, 1998) or to finance terrorism.

Since existing laws and regulations are based on the paradigm that national currency will be used for all relevant local transactions, the existing controls are inadequate to monitor Bitcoin transactions. In addition, many governments have delegated a great deal of the monitoring obligations to the heavily regulated financial system. This measure worked well so far, given that most transactions are settled within the financial system (as a result of the migration from tangible currency – cash – to other forms of payment, such as credit cards, wire transfers, carrier billing etc.). Nonetheless, such controls may prove to be insufficient in a scenario where many transactions are settled outside of the financial system.

Finally, if we assume that Bitcoin is a security, and not a currency, a completely different set of laws and regulations would apply to Bitcoin, such as specific rules regarding registration of issuers, public offerings, mandatory disclosures, suitability, negotiability etc. However, since Bitcoin is not issued by a specific entity, many of those rules would be virtually impossible to apply.

New technologies have generated the ideal conditions for the creation of encrypted private currencies, such as the Bitcoin, The use of such currencies poses many legal challenges in different areas of the law. Prohibition of private encrypted currencies seems precipitated at this moment, given that such currencies are not necessarily associated with criminal activities and may prove useful in the future. This leads to the question as to whether Bitcoin should be regulated (as national currencies are) or left unregulated (as it currently is). There is no consensus regarding the answer to this question and the analysis of this matter should be carried out on a country-by-country basis.

Not regulating encrypted currencies may not be advisable, in view of the particularities and challenges mentioned above. Moreover, the option to maintain encrypted currencies unregulated means, in the end, that regulators, government authorities and courts will have to apply to encrypted currencies the existing laws and regulations, which may not be adequate to deal with such currencies. In some cases, this may even affect the viability of encrypted currencies.

Therefore, regulating private encrypted currencies seems to be a reasonable idea. If regulators decide to follow this path, it will be necessary to deal with many difficulties, such as: (i) how to define such encrypted currencies (should it be treated as currencies, securities or something else); (ii) whether it is a sound policy to break the monopoly of national currencies in a country's jurisdiction; (iii) how to regulate decentralized currencies, which have no particular issuers and are not traded by regulated entities (such as financial institutions); and (iv) how to organize foreign exchange markets, in a context where national currencies coexist with private currencies.

Since the amounts involved in encrypted currencies are still relatively low, most regulators believe that such currencies are not a threat to the stability of the financial system today. Therefore, regulators are adopting a conservative approach and waiting for further developments before deciding on whether to prohibit or regulate encrypted currencies[37]. The next years will determine if encrypted currencies will succeed and become a part of everyone's lives and if regulators will manage to create effective regulations capable of mitigating the inherent risks of such currencies, without affecting its viability.

II. LAW AS META-TECHNOLOGY

A. Theoretical Approach

"Left to itself, cyberspace will become a perfect tool of control."[38]

As explained in the introduction, the second category concerns the law conceived as a meta-technology. One of the perspectives falling within this category

---

[37] See the European Central Bank report, "Virtual Currency Schemes", issued in October, 2012, for a detailed analysis on the current stage of virtual currencies, including encrypted currencies, and the regulators' position regarding the matter. The Central Bank of Brazil has issued the Communication No. 25.306 on 19.2.2014, whereby it has raised a number of concerns associated with "virtual currencies", such as (i) lack of regulation over the currencies and its issuers; (ii) uncertain conversion of such currencies into official currencies or commodities; (iii) risk of having low acceptance in the market; (iv) high volatility, risking total loss of the investment; (v) risk that future regulation worldwide will impact the value of or ability to negotiate the currencies; (vi) risk of being involved in investigations by the authorities, since such currencies may be used for illegal activities; (vii) risk of cybercriminals stealing currency stored in digital wallets, Finally, the Central Bank of Brazil has also indicated that "digital currencies" are not capable of threatening the financial system at the moment, but that it will follow the evolution of such currencies and evaluate the need to regulate it. Available at: < https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=114009277>. Visited on: 6.16.2015.

[38] L Lessig, *Code And Other Laws Of Cyberspace*, 1999.

concerns the situation where the law is needed to limit the impacts of technology, and especially the effects of techno-regulation. The first part of this section describes the relation between technology and law, and the perception of law as a meta-technology. It explains how technology becomes part of decision-making processes, is used to create environments that nudge and steer human behavior, and how this might erode human values. The second part illustrates the possible tension between law and techno-regulation on the basis of copyright protection. Some ten years ago this topic spurred huge debates in Europe. Even though the example is a bit outdated, it is probably the best illustration of the regulatory dilemma addressed in this section.

Machines as subject of communication. A defining feature of today's digital info-sphere is that, the firs time in human history, machines assume the role of subject in communicative processes. In the new digital info-sphere, machines (robots, smart agents, healthcare systems, ambience intelligence, etc. and finally to embrace them all, "the internet of things") not only store, process or disseminate information but they actively take part in the production of "knowledge"[39]. We witness the emergence of autonomous artificial agents (AAs) and further smart environments in which AAs and humans interact at an unprecedented intensity of interconnectivity, communication and feedback (Hildebrandt, 2015). As Hildebrandt puts it, "The thingness of our artificial environment seems to turn into a kind of subjectivity."

Considering that any control procedure or regulative model is also a special type of communication (Wiener, 1989 and Luhmann, 2004), it would not be erroneous to conclude that autonomous AAs will increasingly take part in and eventually dominate the decision making systems of the society (Heylighen, 2002)[40]. As machines turn out to be subjects engaging in communication and thus in the production of "meaning", they also possess the capacity to serve as the "tools of control". From the evolutionary perspective, Law may be regarded as a "technology" which contributes to the more efficient organisation of the society by regulating human behavior.

A new modality of regulation.

In the legal domain, along with the advances in programming and automation which give rise to AAs we witness the emergence a new modality of regulation where AAs' technological capabilities are used to limit and steer human conduct in autonomic environments (Reidenberg, 1998). From the functional standpoint, both technology and Law may act as regulatory mechanisms which seek to subject human conduct to the governance of certain rules (Kelsen, 1942). Technologies are employed to direct human behaviour in a way that assures a patterned outcome[41]. Depending on

[39] Under this new paradigm, we see the demise of the *Cartesian* ontology of legal order where *subjects* are the possessors of rights and *objects* are the property subordinate to legal subjects. The future society, as steered and automated by the predictive algorithms, will witness the further blurring of the subject/object dichotomy. As machines become more autonomous, they will imitate human cognitive qualities at such a level that their entitlement to "personality" will not possibly be negated by orthodox legal discourse.

[40] The current post-industrial society, with increasing automation and algorithmic regulation, seems to be heading to a cybernetic social order.

[41] Apart from law and technology, market forces and social interaction also have a normative

the context, such regulatory models may interchangeably referred as: "regulation by technology", "technological normativity", "regulative software", "techno-regulatory systems", "law as design" or "algorithmic regulation".

Techno-regulatory settings may focus on products/services, places or persons (Madison, 2005). Today we commonly experience techno-regulatory applications in products and services (speed limiters in cars, internet filtering, personalised information services etc.). Regulation by technology in the spatial realm may be referred as "ambience intelligence" where speed monitoring, CCTV cameras, smart buildings, face recognition software together with wearable computing technologies are the pioneer examples. The deployment of techno-regulatory tools targeting persons is a near future scenario where the desired course of conduct will be wired to human beings either by way of genetic manipulation, administering of drugs or by other means that might be used to alter brain functioning (Burk, 2002).

Theoretical implications of regulation by technology.

This new modality engendered through regulative capacitates of algorithms, predictive analytics and their recombinant effects results with the eradication of the moral ground, the normative enterprise, and the chain of causality as understood in the conventional legal systems (Custers, 2013). The question here is not whether law could be reduced to formal logic and thus fully embodied in computer programs. Rather it is that, computational machines have an intrinsic normativity that could deliberately eliminate certain choices of action and thus indirectly dictate the desired behavior.

In a techno-regulatory setting, law operates at a higher level of order as "meta-technology" so that, we witness the emergence of legal norms which no longer command human conduct but regulate the design of the systems that limit, shape and govern the society[42] (Pagallo, 2013).

Demise of law as a normative enterprise.

In a techno-regulatory setting, there are three-phases of legal process that can be referred to as: direction (rule making), detection, and correction. They collapse into each other and become an opaque embedded inner process. Where technology is used to steer human conduct with a view to ensure compliance with certain norms, the regulatory regime loses its normative character since non-compliance is made impossible through design choices. At this point, our thinking of law departs from "should/should not" to "can/cannot". What is not legal also cannot be done (Brownsword, 2011). Techno-regulatory systems deprive individuals of the ability to reason with the rules and accordingly the capacity to decide what ought to be done.

Moral enterprise: Free will, liability and autonomy.

Using technology to attain control that is beyond the possible limits of a

impact. *See* Madison (2010) and Lessig (1999).

[42] The issue of level of abstraction and control order is also elucidated by Turchin (1977) under the concept of meta-system transition in relation to systems theory and cybernetics.

conventional legal system, would eradicate human freedom and accountability because one would be left without alternative choices of action (Hildebrandt, 2008). Liability, as a reflection of moral basis of law is also going under a transformation owing to the increasing social and administrative complexity resulting from the pervasive deployment of ICTs. The hyper-complexity we are heading through obscures the specific source of liability so that some scholars speak of a new "distributed morality" (Floridi, 2015).

Secondly, as tools for prediction and prevention become more potent, we will end up with a social order where the sole liability shall rest with the governing systems (Simon, 2015). The perceived omnipotence of techno-regulative systems will result with an expectation to predict and prevent any eventuality or wrongdoing. In such scenario, humans will probably lose their ability of anticipation as well as the feel of common sense. The conventional legal systems[43] always maintain a margin of autonomy, which requires the conscious and anticipative participation of the moral subjects.

Predictive algorithms deployed by the techno-regulatory systems also transform criminal law in such a way that the principles of retribution and moral liability are becoming replaced with prediction, crime prevention and risk management - a "Minority Report" scenario -. The individual is considered as a risk object and thus not as a blameworthy moral subject.[44] As criminal law becomes the "law of prevention", citizens lose the legal safeguard of the most important principle: nullum crimen nulla poena sine lege.

Breaking the chain of causality: the reign of correlations. Techno-regulatory systems increasingly act on correlations derived by way of data-mining techniques and predictive analytics. While conventional law relies on facts provable by natural rules of causation, in a techno-regulatory setting we observe a shift from "facts" to "correlations". Application of rules follow an automated procedure based on algorithmically pre-defined correlations (Hildebrandt, 2008). This phenomenon, which may be described as a kind of "social alchemy", raises questions that it is prone to manipulation, and may lead to a selective application of the law (Hildebrandt, 2013).

The accuracy or the truth attributed to data mining practices is not due to any correspondence to a pre-existing reality, but rather reality is constructed by way of correlations detected through data mining. These 'blind correlations' do not stem from predefined hypotheses and do not conform to the principle of cause and effect. Irrespective of the fact that inferred correlations do not submit to the principle of causation, they nevertheless serve as the basis for decisions concerning marketing, management, finance, security, crime investigation, medical research and credit rating (Hildebrandt and de Vries, 2013).

---

[43] Conventional legal system described by Pagallo (2015) as: "(i) made of commands; (ii) enforced through physical sanctions; (iii) within the territory of a sovereign state."

[44] Pagallo, *The Laws of Robots Crimes, Contracts, and Torts*, 8.

The rule of law and human autonomy.

Diminishing the legal system to a series of intricate information processes which mainly act on correlations rather than "facts", challenges law's claims to rationality, objectivity, neutrality, autonomy, and universality at various levels and contexts. The notion of legitimacy in a democracy depends on the fact that individuals are free to choose among alternative courses of action rather than being free to decide in what manner they would restrict their freedom. While setting the criteria in order to assess techno-regulation, the primary notions would be human rights with a view to maintain a critical approach (Brownsword, 2011). However this substantial criteria based on human rights is of little help if not reinforced by certain procedural mechanisms and principles e.g., inclusive participation, transparency and accountability (Koops, 2007).

Where non-normative instruments dominate the regulatory environment, we seem to be subject to the rule of technology rather than the rule of law. Techno-regulation signals the demise of our capacity to reason against and resist, and thus it may result with a further deviation from the values that make us "human". As elegantly put by Oscar Wilde (1891): "Disobedience, in the eyes of any one who has read history, is man's original virtue. It is through disobedience that progress has been made, through disobedience and through rebellion."

B. *Practical Approach:* **the struggle for enforceable copyrights**

The above clearly illustrates how technology can erode human rights and values, taking us as far as a minority report scenario where prediction on the basis of correlations steer and judge our behavior, in stead of democratic rules and proven facts. Koops and Hildebrandt (2010) have already criticized this undesired scenario. They suggest that a model exclusively based on techno-regulation could harm the concept of free will, because it enforces the law without any room for human reason. Moreover, there is a problem with democratic legitimization as technological development depends upon market forces instead of legislative initiatives. As already addressed above, such approach replaces the rule of law by a "rule of technology". According to Koops and Hildebrandt (2010) technology must comply with at least two important requirements in order to become law: democratic legitimacy and the possibility of contestation in a Court of law. The influence of technology on law, and the need to balance such influence by legal intervention, will be illustrated below on the basis of the struggle for enforceable mechanisms of copyright protection.

How technology can decide legal judgment.

Even though modern file-sharing has its origin in the 2000s, this era is also known for peak sales of CDs and DVDs.[45] While the technological characteristics of

[45] For the United Kingdom, see: http://www.dailymail.co.uk/sciencetech/article-1270704/DVD-sales-decline-likely-die-internet-Digiboxes-over.html/. For the US it is stated

file-sharing software turned out to be decisive for legal qualifications and enforcement, for cd's and DVDs the regulatory table was turned from legislation to techno-regulation, and back. Both examples illustrate the severe impact technology has on steering behavior, and the delicate balance the law must safeguard in protection against unwanted or even illegal behavior on the one hand, and the protection of fundamental rights and values on the other hand.

Interesting in the case law against file-sharing service Napster was the technological architecture of this service making it quite easy for a judge to shut down the entire system. The use of a centralized structure where indexing and searching is performed on Napster servers lead to a situation where individual files were only downloaded from this central server. Because of this structure a judge could simply file an injunction, forcing Napster in 2001 to shut down its network. Immediately after, other file-sharing software became popular under the name peer-2-peer software. In this scenario the technological architecture is not one central server from which a multitude of people can download a multitude of (copyright protected) works, but a system of dispersed servers by using the computers of file-sharers as a combined network of servers, linked together by the installation of a piece of peer-2-peer software. This architecture lead an appeals court in the US to rule that file-sharing software such as Grokster and Morpheus is legal because the makers did not have control over the servers on which it ran (Heins, 2003).

In retrospect we all know now that eventually Grokster was held liable because of inducement, but not because the software as such was deemed illegal, as legal usage of the technology is a possibility.[46] Even though file-sharing of copyright protected material is illegal, the characteristics of the technology - sharing of dematerialized goods at a global scale - bear all kinds of difficult legal questions both regarding material and procedural issues. Can you steal an intangible good? As in fact you do not take the good out of possession of person A to bring it into possession of person B, but you make a copy, leading to both person A and B having possession of the good. Procedural issues mainly concern questions regarding applicable laws and competent courts, and how to enforce foreign verdicts, related to the fact that offshore P2Ps are being set up in specific locations so as to take advantage of less restrictive copyright laws and weaker judicial enforcement mechanisms.

If the law can't fix it, technology can. The issue of enforcement of rights also played an important role in another copyright related debate. Regardless of there being laws against copying CDs and DVDs, this has been common practice ever since these carriers of popular music and films were put on the market. The copying culture might have to do with the fact that people do not consider copying as severe as steeling, it could also be because of the risk of getting caught being low, or simply because the economic benefits of copying outweighs the risk, or even because of

---

that the sales of digital albums first surpassed the sales of physical albums in 2011, http://www.billboard.com/biz/articles/news/digital-and-mobile/5901188/cd-album-sales-fall-behind-album-downloads-is-2014-the

[46] MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005)

penalties - or the chance of them being actually enforced - being low.

Whatever the reason for the copying culture, it is not surprising that the entertainment industry explored different options to fight illegal copying. One particular efficient solution was found in technical copyright protection mechanisms, disabling the opportunity to make a copy of a cd or dvd altogether. From the perspective of producers at first glance a golden opportunity, as the technical measures - as opposed to the law - did not leave room for disobedience.[47] However, from a consumer perspective at least two important disadvantages of such technical protection mechanisms can be mentioned, both relevant to the producer perspective. First, such technical measures quite often prevented playing a CD or DVD on an older or less sophisticated player. This annoying side effect may very well lead consumers to opt for CDs or DVDs without technical protection, an important competitive consideration for suppliers of entertainment if not all choose to equip cd's and dvd's with such mechanism. Second, these mechanisms also spurred debate from a more fundamental legal perspective, especially in Europe in view of the Copyright Directive. This Directive grants rights holders the "exclusive right to authorize or prohibit direct or indirect, temporary or permanent reproduction" of their works. However, the Directive enables EU member states to introduce a range of exceptions to this general rule. One of those exceptions, enacted in the laws of some member states, allows individuals to make reproductions of copyrighted material for non-commercial private use. This is on condition that rights holders receive "fair compensation" to account for lost revenues.

On the basis of this legal right to a private copy, it has been claimed, and sometimes with success, that technical protection mechanisms were in conflict with the law, and thus not allowed. Meaning that the law intervened too far-reaching consequences of technology, and was reinstated as the main modality to protect against copyright infringements, at least as far as copying CDs and DVDs is concerned.

III. TECHNO-REGULATION

A. Theoretical Approach

(GAP)

B. Practical Approach: the digital public sphere in Brazil

The combination of digital technology and the Internet infrastructure

[47] Only few people were knowledgeable enough to circumvent such protection mechanisms, something also penalized by law.

resulted in a medium with huge democratic potential[48]. Adding up new architectural features, the Internet enables multidirectional communication, instant response, expanded possibilities of discourse and debate. Nevertheless, such potential can considerably diminish, depending on how technology layers on top of the infrastructure are built, permitting more or less actions by users and depending on the criteria of accessing and filtering content and discourses by its algorithm[49]. In the process of enhancing political engagement by citizens through new technologies, in the wake of what has been called "e-democracy" or "digital democracy"[50], we must deepen the debate on how this potential is being affected by what we call "techno-regulation".

In the Brazilian context, only recently we can talk about a true widespread usage of the internet. The latest CETIC Households[51] report refers to 49% or 81 million of Brazilian Internet users in 2012, a figure that rises to 74% among those aged from 16 to 24 years. Concerning internet usage for democratic purposes, we are witnessing a moment of several novelties in the country: the 2012 elections consummated the first time that the Internet was used intensively by citizens and candidates in an election campaign, while the protests of June 2013 were the first great cycle of marches in which the use of the Internet played a significant role, demonstrating all of its potential.[52]

---

[48] Considering the characteristics raised by cyberoptimistics like Castells and Benkler, we can say that the new information and communication technologies has been seen as the great democratic promise. With several channels of participation, deliberation, mobilization and transparency, they are considered capable of enabling deeper interactions between society and the system through more communicatively efficient public spheres and greater democratic potential. (BENKLER, 2006; CASTELLS, 1999).

[49] With some differences varying according to their own conceptions of what would be the Internet and research focus, so-called cyber-skeptics share common concerns. Andrew Keen; Nick Carr; Cass Sunstein; Richard Wurman; Mark Bauerlein; Steve Talbott; Jaron Lanier; Matthew Hindman; Sherry Turkle; Evgeny Mozorov; Eli Pariser and Tim Wu are names that, at some point, have been or are associated with this current, each with a particular look with skepticism doses for specific aspects or reticent in general about the democratic potential of the Internet. Eli Pariser, for instance, analyses the democratic loss generated by the invisible filter that puts us in a bubble where everything pleases, everything makes sense, everything is in line with our views and realities. These mechanisms, increasingly sophisticated, imprisons us showing most of the time informations that we agree, depriving us of dissonant voices. (PARISER, 2011)

[50] Scholars like Castells and Archon Fung have identified the impacts generated by the Internet on the mechanisms of (i) improvement of transparency in the political process, by monitoring the performance of government agents and public resources, (ii) facilitation of direct involvement and participation in political processes, and (iii) improvement of the quality of opinion formation by opening new spaces of information and deliberation. (FUNG, 2003; CASTELLS, 2007)

[51] http://cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2012.pdf.

[52] The experience of June 2013 riots in Brazil showed deep institutional problems of legitimacy in our political system, while demonstrating at the same time all the communicative and democratic potential of the new information and communication technologies and the network organizational culture. There was at this time the embryo of a truly connected active public sphere, representing a breakthrough because of the potential the Internet found in these

Also, the prioritization of Internet access and the necessity to improve its use for democratic purposes, claims that are being echoed in the Brazilian public sphere, have found representation in recent legislation. In its Article 7, the Brazilian Civil Rights Framework for the Internet[53], a law that resulted of a public consultation through the Internet started in 2009 and approved by the Congress in 2014, determines that "Internet access is *essential* to the exercise of citizenship (...)"[54]. Moreover, in 2011, the Access to Information Act (Law no. 12.527)[55] was approved, establishing mechanisms for mandatory disclosure of open data mainly via Internet, as well as online requests for information by any citizen, aiming to promote maximum transparency in public administration. From the point of view of public policy, the National Broadband Plan[56], launched by the Ministry of Communications in 2010, determined quantitative targets and guidelines to stimulate the expansion of access in Brazil for the next years.

It becomes apparent that Brazilian government and citizens perceive the potential of the connected public sphere in Brazil and how it is playing an important role in the digital age in terms of access to knowledge, access to information, free spreech and accountability (Faria, 2012).

However, a new scenario starts to be built on another direction, fast and invisibly. Although Internet regulations in Brazil – such as the Brazilian Civil Rights Framework for the Internet - seek to value the Internet's democratic potential and regulate practices aiming to protect constitutional rights, the auto-regulation based on

---

spaces. The role of online alternative media, the advantage of speed in the communicative flow in digital platforms, the ability to quickly mobilize and organize on social networks are all unprecedented elements and mechanisms that were crucial in this period of social upheaval and illustrate the democratic potential of the Internet.

[53] In Portuguese: Marco Civil da Internet. Officially Law No 12.965. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

[54] The project bill of "Marco Civil da Internet" was set in a context in which Brazilian representatives, academics and civil society organizations have worked together to bring more legitimacy and participation in the process of creating laws through the use of Internet platforms. The draft represented a commendable state initiative to expand the debate and communication skills in the preparation of rules. The online public consultation promoted by the Government, incremented the debate in the public sphere opening channels for discussing the content and procedures of the rules aiming a greater acceptance of the law. However it is important also to see beyond the process` merits. This deliberative process, despite being commendable and novel in Brazil, also experienced limitations to its potential, for instance, not all expressions were contemplated due to challenges such as lack of Internet access, the effects of technicalization of debate and the strong lobby imposed by some private sectors. Nevertheless, considering that it was the first experience of legislative online consultation in Brazil, it has already been a good advancement. But it is important that in the next similar processes both civil society and government try to correct these flaws and make viable all possible resources for digital inclusion and capacitate citizens for the debate, expanding the capacity to absorb the expression of all possible affected by the rule.

[55] http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.

[56] http://www.mc.gov.br/programa-nacional-de-banda-larga-pnbl.

design simply surpasses the regulation of law, subverting the traditional "should/should not" logic of the rule of law and establishing the logic of "can/cannot" of a new "rule of technology", leaving no alternative choices of action for citizens or governments.

In practical terms, the Brazilian Civil Rights Framework for the Internet establishes a safe harbor[57] for Internet Service Providers and strongly declares the importance in ensuring free speech in the cyberspace. Nevertheless, algorithms regulation can automatically and invisibly filter, censor and remove content, which may go unnoticed and without penalty. As stated in the introduction of this paper, "in a techno-regulatory setting, rules no longer embody the politics that they are based on, but they simply dictate it".

The mechanism of techno-regulation used by Youtube through its Content ID[58] system severely jeopardizes the Brazilian remix culture coming from Funk[59] and Tecnobrega[60] expressions in the music scene. Facebook's algorithms aimed at filtering pornography have recently censored a picture posted by the Ministry of Culture in Brazil in its official Facebook page depicting two Brazilian natives. Given the lack of transparency of automatic filtering and the indifference demonstrated by the Facebook in this latter case, The Brazilian Minister of Culture publicly declared that the algorithmic private censure was abusive, violating the rights to sovereignty and access to culture, demanding more explanations by the company and threatening them with possible judicial prosecution. [61]

Both examples give us a clear perspective that the techno-regulation is already an established practice and is being used to attend exclusively to commercial purposes without any concern of observing constitutional rights or specific Internet regulations. Although Brazilian policy makers and citizens are aware of the democratic potential of the Internet, they are not sufficiently aware of the risks that are coming together in this scenario promoted by private companies. To avoid a techno-regulation scenario where the rule of law is overruled by algorithms, superimposing civil and constitutional rights, we must seek a more effective regulation of these technologies, from a meta-technology perspective of the law.

Considering the importance of the law as an effective system to regulate actions, and also considering that its criteria rightly preserves individual freedom to choose among alternative courses of action preserving human autonomy, techno-regulation needs to be guided by the rule of law, considering law as a meta-technology that orients regulation by technology. To optimize the positive effect and minimize the damage brought by the disruptive effect of technological advanced regulation, it is

---

[57] Brazilian Civil Rights Framework for the Internet states, with some exception, that Internet Service Providers are only obligated to remove content by means of judicial decision.
[58] https://support.google.com/youtube/answer/2797370?hl=pt-BR
[59] https://en.wikipedia.org/wiki/Funk_carioca.
[60] https://en.wikipedia.org/wiki/Tecno_brega.
[61]Http://www.cultura.gov.br/noticias-destaques/asset_publisher/OiKX3xlR9iTn/content/id/1248553.

crucial to understand their impacts and consequences, considering the technical aspects and peculiarities of the new forms of communication and also regulation.

Private companies have a relevant role in the enforcement of constitutional rights in the connected public sphere. Without obligation to revise eventual abusive and non-informed algorithmic filtering and removal of content or their reasons to the public scrutiny, there is no public control over such practices. The challenge, as such, is to observe these practices and measure their importance in political and social communication and guide the technology by a more efficient law regulation in a way that it preserves user's autonomy. As Hartmann (2015) puts it, the law as a meta-technology, must try to reverse this scenario aiming to superimpose the dominance of design by imposing more specific and severe duties concerning virtual democratic spaces.

IV. A FINAL CASE STUDY AND FINAL REMARKS: BLURRED LINES?

The Dodd-Frank Act, and in particular Title VII of the Act, provides an interesting example of the interplay between law, technology and business drivers in the arena of the financial markets. [62] In particular, we focus on the relevant parts of the Act pertaining to the regulation of the Swaps market, a market that has undergone major transformations due to rapid technological progress.[63]

Dodd-Frank blurs the distinction between Law as a Meta-Technology and as a Techno-Regulation. In the context of Dodd-Frank, evolving Technology is at once a cause of the problems, the enabler of the solution and the enforcer of the regulation. We argue that the Act seeks to enforce its goals via design of the technology. It also leverages the voluntary mutual interest of market participants with standardization of technology to self-enforce compliance and as such serves as an interesting case study.

Background: The 2008 Financial Crisis and the Dodd-Frank Act.

---

[62] The Dodd-Frank Wall Street Reform and Consumer Protection Act, 124 Stat. 1376 (2010). For a brief overview by the banking committee: http://www.banking.senate.gov/public/_files/070110_Dodd_Frank_Wall_Street_Reform_comprehensive_summary_Final.pdf; For a brief review of Title VII of the Dodd-Frank Act, the Wall Street Transparency and Accountability Act of 2010, see: http://media.mofo.com/files/uploads/images/summarydoddfrankact.pdf. Similar regulation is undergoing in the UK and Europe. For an overview, see Greenberger (2011). The CFTC and SEC implemented Title VII with the "Final Rule": http://www.cftc.gov/ucm/groups/public/@newsroom/documents/file/federalregister071012c.pdf. However, the implementation of Dodd-Frank is not yet near its completion.

[63] Dodd-Frank reformed much of the American financial markets and its regulations span diverse areas including mortgages, consumer banking and regulatory bodies' structure. In this paper, we focus on the regulation pertaining to trading certain types of derivatives (Title VII).

The American Congress blamed the Over the Counter (OTC) Derivatives market - and in particular the enormous OTC Swaps market - as one of the main causes of the financial meltdown that culminated in the 2008 collapse of Lehman Brothers and the ensuing global recession that followed.[64] The fuse that lit the bomb was the Credit Default Swaps market. Its highly leveraged and speculative nature caused great losses to many financial institutions and brought them to the brink of insolvency. The interconnected nature of the long-term mutual commitments embedded in the broader swaps market caused the US government to fear systemic failure. The government feared that a financial behemoth's collapse would drag down the rest of the financial institutions with it. Indeed, after Lehman's bankruptcy, the US government infused money to the system under the TARP program and ensured that no other major institutions will fail.

In the aftermath of the crisis, Congress enacted the Dodd-Frank Act with the following goals: (1): increase transparency and efficiency in what Congressmen deemed an opaque and inefficient market place; (2) reduce systemic risk by reducing the risk that a firm would be "too big to fail" lest it bring down the market with it; (3) bring regulation and oversight into a lightly regulated market; and thus (4) provide tools to the US government's regulatory bodies to independently assess the market-wide as well as firm-specific risks.

To that end, the Act decreed, *inter alia*, that to enhance transparency and efficiency the following steps were needed: (1) Certain derivatives instruments - and in particular certain types of Swaps - traded by particular parties be electronically traded on newly regulated Swap Execution Facilities known as SEFs; (2) The SEFs should electronically post the requests for quotes (RFQ's) and provide a minimum number of quotes for each such request; (3) The trades should be electronically reported to designated reporting depositories in quasi-real time and be made available to government's scrutiny. Furthermore, to reduce systemic risk due to "too big to fail" players, the Act requires that the clearing and settlement of certain trades be done via special Central Clearing Houses and not as bi-lateral obligations between the trading parties as done heretofore.

Technology as a Cause of the Problem.

Technology changed the market dynamics and created an environment rife with new risks and market failures. Swaps are complex long term contracts, whose details are set in an ISDA Agreement and its schedules[65]. Pricing a swap involves

---

[64] According to the Bank of International Settlements, at the end of December 2014, the total outstanding notional value of derivatives (excluding options and futures) exceeded 500 trillion USD. See http://www.bis.org/statistics/dt1920a.pdf. Congress and Academia blamed other factors as well.

[65] Swaps refer to a wide variety of derivatives whose main mechanism is the swapping of one financial asset for another based on agreed terms and conditions. The simplest of swaps is an Interest Rate Swap, where the two parties agree to exchange periodic interest payments on a hypothetical loan, where typically one side would pay a fixed interest rate (fixed leg) whereas the other side pays a rate indexed to some benchmark index such as LIBOR or Prime rate (floating leg). *See* FABOZZI & MANN (2012).

complex math which increases in complexity as the creativity of the counterparties deviate from its original form. Even the simplest of Swaps, a Vanilla Interest Rate Swap (IRS), is governed by an ISDA Agreement comprising tens of pages. Individual Swap Transactions are described in schedules that can span many detailed pages themselves. Thus, the operational overhead associated with processing these trades is extensive. Furthermore, the management of the Swap over its life time typically involves dozens of payments over many years and traditionally required significant manual labor. The complexity of the agreements and the intensive labor associated with them limited both the volume of the transactions as well as the complexity of the agreements.

In the last twenty years, mathematical computational power evolved to allow quants and traders to price and trade increasingly more complex swaps. Furthermore, data processing technology evolved to represent and handle efficiently the intricate details of swaps and thus enabled a rapid growth in trading volume. To demonstrate the rapid technology-enabled growth, the market in the simplest of the swaps, the Interest Rate Swaps, has grown in volume from less than USD200B in daily turnover in 1995 to over a Trillion USD in 2004 and reached more than 1.6 Trillion USD a day by April 2007. Were it not for the size of the market, the extent of the long-term commitments and the number of parties interconnected in these contracts, the crisis could have likely been averted. As such, one may view technology as one of the causes of the 2008 financial crisis.

Technology as the Enabler of the Solution.

Dodd-Frank's reform of the derivatives market relies heavily on technology's ability to support its requirements in every stage of the proposed restructuring of the market. (1) Only recent technological advances in communication, computation and standardization of protocols enabled the creation of the **SEF's** that serve as the basis of the reform[66]. (2) Without the technical ability to electronically process the clearance and settlement of the trades, **clearing houses** could not take on the challenges of handling swaps. The manual labor required for such processing would have made it impractical. (3) The evolution in the electronic representation of the trades enabled the government to collate the data in standardized formats into the **reporting depositories**. (4) Finally, without the quantum leaps in computational power, the government could not expect to process the vast amount of data, slice and dice it internally and perform complex risk analysis. It would have had to continue to rely on inadequate self-reporting procedures and couldn't exercise the **oversight and risk management** it outlined in the Act.

Technology as the Enforcer of the Solution.

Most interestingly, technology is also the enforcer of the reform. Dodd-

[66] It is interesting to note, that technology also served as a negotiation tool by Wall Street in justifying its resistance to certain proposed measures. The Wall Street firms argued they do not possess the necessary technology to implement certain provisions. Indeed, much of the Dodd-Frank reform has been delayed due to firms' failure to develop the necessary technology.

Frank essentially created an **entirely electronic eco-system** that encompasses all stages in the life cycle of a Swaps trade: The cycle starts with a trader posting an Electronic Request for Quote on an all-electronic SEF. Market makers provide electronic quotes and consummate the trade electronically on the SEF. The parties and the SEF report the details electronically to the Reporting Depository. At the same time they electronically forward the trade details to the Clearing House for clearance and settlements.

As such, the Act dictates certain design requirements to the developers of all the related systems so that they interoperate and be compatible with each other. However, this goes deeper, by creating this all-electronic eco-system Dodd-Frank enforces compliance as well. A rogue trader who will try to trade outside the regulated electronic eco-system will be hard pressed to find American counterparties willing to trade with him. Trading outside the all-electronic environment would be labor intensive and highly inefficient, and thus few firms would venture to trade outside the framework. Furthermore, even if an occasional rogue trade were to occur outside the system, it would not be of significant importance and its impact will be limited. Compliance is further enforced by the mutual need to follow the rules in the implementation phase as well. A firm that chooses to "play" in the eco-system but fails to follow the details of the implementation will find it cannot "fit in" and thus be forced to upgrade its systems into compliance with the standards and protocols used in the eco-system by the other players.

To conclude, the Dodd-Frank act sheds an interesting light on the interplay between law, technology and business. US Congress enacted Dodd Frank to address a problem in the derivatives market that was caused, among other factors, by technical advances. The solution proposed by Congress relies on evolving technology and could not be implemented until the required technology needed to support became widely available. Finally, the reform relies on the creation of a predefined all-electronic system in which trading, settlement and regulatory oversight all take place to enforce compliance. The power of the eco-system lies in the fact that all parties must adhere to common protocols and standards lest they find themselves stranded "outside" the system and unable to transact business with the parties "inside". Thus, it is not only regulation that forces compliance but also the mutually aligned common interests of all players to cooperate in creating a standardized compliant eco-system. In this respect, Dodd-Frank blurs the distinction between Law as meta-technology and Techno-regulation yet gives insight to both perspectives.

(FINAL REMARKS)

REFERENCES

ALTAM, E. J.; TRIPSAS, M. (2015), Product-to-Platform Transitions: Organisational Identity Implications" In: ZHOUU, J. *et al.*, (Eds.) *The Oxford Handbook of Creativity, Innovation and Entrepreneurship*. Oxford: Oxford University Press.

BAKOS, Y. and DELLAROCAS, C. (2011), Cooperation without Enforcement? A Comparative Analysis of Litigation and Online Reputation as Quality Assurance Mechanisms. *Management Science*, 57(11), 1944-1962.

BALWIN, C.Y; WOODARD, C.J. (2009), The Architecture of Platforms: A unified view In: GAWER, A. (Ed.), *Platforms, Markets and Innovation*, Vol. 1. England: Edward Elgar.

BISWARUP, G.; JAYADEVAN, PK.; BHARAT, J. (2014), *Brands cry foul over counterfeit products on e-commerce sites like Flipkart, Snapdeal, Amazon and others* (December 03, 2014). Available at: http://articles.economictimes.indiatimes.com/2014-12-03/news/56684849_1_snapdeal-counterfeit-goods-vivek-prabhakar (Accessed on June 12, 2015).

BROWNSWORD, R. (2011). Lost in Translation: Legality, Regulatory Margins, and Technological Management. *Berkeley Technology Law Journal*, Vol. 26, No. 3.

BURK, D. L. (2002) Lex genetica: The law and ethics of programming biological code, *Ethics and Information Technology* 4**:** 109–121.

CHIODI, G. M. (2000). *Equità. La regola costitutiva del diritto*. Torino: Giappichelli.

CUSTERS, B., et al. (2013). *Discrimination and Privacy in the Information Society, Data Mining and Profiling in Large Databases*. Springer-Verlag Berlin Heidelberg.

DURANTE, M. (2008). What Model of Trust for Networked Cooperation? Online Social Trust in the Production of Common Goods (Knowledge Sharing). In: T. Ward Bynum, M.C. Calzarossa, I. De Lotto, S. Rogerson (eds.). Living, Working and Learning beyond Technology. *Proceedings of the Tenth International Conference Ethicomp 2008*, 211-224, Mantova: University Press.

DURANTE, M. (2010). What Is the Model of Trust for Multi-agent Systems? Whether or Not E-Trust Applies to Autonomous Agents. *Knowledge, Technology & Policy*, 23(3-4), 347-366.

EUROPEAN CENTRAL BANK. *Virtual Currency Schemes*. October, 2012.

FABOZZI, F. J.; MANN, S. V. (2012) The Handbook of Fixed Income Securities, 8th ed.

FARIA, C. F. S. (2012) *O Parlamento aberto na era da internet: pode o povo colaborar com o legislativo na elaboração das leis?* Brasília: Ed Câmara, 2012.

FLORIDI, L. (2015) (Ed.) *The Online Manifesto: Being Human in a Hyperconnected Era*. London: Springer.

GLADSTONE, J. A. (1997) Exploring the Role of Digital Currency in the Retail Payments System. 31 *New Eng. L. Rev.* 1193.

GHANEA-HERCOCK, R. (2007). Dynamic trust formation in multi-agent system. *Tenth international workshop on trust in agent societies at the autonomous agents and multi-agent systems conference* (AAMAS 2007), Hawaii; May 15, 2007. Available at: http://www.istc.cnr.it/T3/trust.

GREENBERGER, M. (2011) Overwhelming a Financial Regulatory Black Hole with Legislative Sunlight: Dodd-Frank's Attack on Systemic Economic Destabilization Caused by an Unregulated Multi-Trillion Dollar Derivatives Market, 6 *J. BUSINESS & TECHNOLOGY LAW* 127.

GRINBERG, R. (2012) Bitcoin: an innovative alternative digital currency. 4 *Hastings Sci. & Tech. L.J.* 159.

GRODZINSKY, F. S.; MILLER, K. W.; WOLF, M. J. (2010). Developing artificial agents worthy of trust: Would you buy a used car from this artificial agent? *Proceedings of CEPE*, June 2009, Greece.

HARTMANN, I. (2015) A auto regulação pelo código: características, impacto e limites de um novo modelo.

HEINS, M. (2003) *The progress of Science and Useful Arts*: Why Copyright Today Threatens Intellectual Freedom. Available at: http://www.fepproject.org/policyreports/copyright2d.pdf

HEYLIGHEN, F. (2002). The Global Superorganism: an evolutionary-cybernetic model of the emerging network society*, Journal of Social and Evolutionary Systems,* Available at: http://pespmc1.vub.ac.be/papers/superorganism.pdf.

HILDEBRANDT, M. (2008) Legal and Technological Normativity: more (and less) than twin sisters, *Techné: Research in Philosophy and Technology*, 12:3.

HILDEBRANDT, M. and KOOPS, B-J. (2010) The Challenges of Ambient Law and Legal Protection in the Profiling Era. *Modern Law Review*, Vol. 73, Issue 3, pp. 428-460, Available at SSRN: http://ssrn.com/abstract=1602192 or http://dx.doi.org/10.1111/j.1468-2230.2010.00806.x

HILDEBRANDT, M. (2013) *Slaves To Big Data: Or Are We?*, Keynote 25th June 2013, 9th Annual Conference on Internet, Law & Politics (IDP 2013, Barcelona).

HILDEBRANDT, M.; VRIES, K. (2013) *Privacy, Due Process and the Computational Turn*. New York: Routledge.

HILDEBRANDT, M. (2015). The Public(s) Onlife: A Call For Legal Protection by Design. In: FLORIDI, L. (Ed.) *The Online Manifesto: Being Human in a Hyperconnected Era*. London: Springer.

HOFFMAN, C. D. (1998). Encrypted Digital Cash Transfers: Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations. 21 *Fordham Int'l L. J.* 799.

HURWITZ, J-G. (2013). Trust and Online Interaction. *University of Pennsylvania Law Review*, vol. 161, 1579-1622.

LOCKTON, D.; HARRISON, D. J.; STANTON, N. A. (2010) The design with intent method: a design tool for influencing user behaviour, *Applied Ergonomics*, 41(3): 382-392.

MACINTOSH, Kerry L. How to Encourage Global Electronic Commerce: The Case for Private Currencies on the Internet. 11 *Harv. J. L. & Tech.* 733.

MADISON, M. J. (2010). Law As Design: Objects, Concepts, And Digital Things, *Case Western Law Review*, Vol. 56, No. 2, 2005.

MATTA, V. and FROST, R. (2011), *Motivations of Electronic Word-of-Mouth Communications by Reviewers*: A Proposed Study (August 8, 2011), 1-6. Available at SSRN: http://ssrn.com/abstract=1906919.

NISSENBAUM, H. (2004). Will security enhance trust online, or supplant it? In R. M. Kramer & K. S. Cook (Eds.). *Trust and distrust in organizations: Dilemmas and approaches* (pp. 155–188). New York: Sage.

KAPLANOV, N. M. (2013). Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against its Regulation. 25 *Loy. Consumer L. Rev.* 111.

KARE-SILVER, M. (2014) *Digital Insights 2020*: how the digital technology revolution is changing. England: Troubador.

KELSEN, H. (1942) The Law As A Specific Social Technique. 9 *University Of Chicago Law Review* 75-97.

KOOPS, B. J. (2006) Should ICT regulation be technology-neutral?, in *Starting points for ICT regulation: deconstructing prevalent policy one-liners*, pp. 77-108. B-J. Koops et al. (Eds.), The Hague, TMC Asser.

KOOPS, B. J. (2007) Criteria for Normative Technology: An Essay on the Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values. In: BROWNSWORD; YOUNG (Eds.) Regulating Technologies. Oxford: Hart Publishing; TILT Law & Technology Working Paper Series No. 005/2007

KOOPS et al. (2010). *Dimensions of Technology Regulation*. Nijmegen: Wolf Legal Publishers.

LUHMANN, N. (2004). *Law as Social System*. Oxford University Press.

OECD. (2010) *Economic models and role of Intermediaries in the Value Chain* (April 2010) Available online at : http://www.oecd.org/internet/ieconomy/44949023.pdf (Accessed on June 12, 2015).

PAGALLO, U. (2012) Cracking down on autonomy: three challenges to design in IT law, *Ethics and Information Technology*, 14(4): 319-328.

PAGALLO, U. (2013) *The Laws of Robots Crimes, Contracts, and Torts*. Dordrecht: Springer Science+Business Media.

PAGALLO, U. (2015) Good Online Governance: On Law, Spontaneous Orders, and Design. In: FLORIDI, L. (Ed.) *The Online Manifesto: Being Human in a Hyperconnected Era*. London: Springer.

REIDENBERG, J. (1998). Lex Informatica: The Formulation of Information Policy Rules through Technology , 6 *Tex. L. Rev*. 553.

RESTA, E. (2009). *Le regole della fiducia*. Roma-Bari: Laterza.

SARKAR, J. (2015) *Shopping Online? Beware of Fakes* (January 19, 2015). Available online: http://timesofindia.indiatimes.com/tech/tech-news/Shopping-online-Beware-of-fakes/articleshow/45934537.cms (Accessed on June 12, 2015).

SCILLITANI, L. (2007). *Fiducia, diritto, politica. Prospettive antropologico-filosofiche*. Torino: Giappichelli.

SIMON, J. (2015) Distributed Epistemic Responsibility in a Hyperconnected Era. In: FLORIDI, L. (Ed.) *The Online Manifesto: Being Human in a Hyperconnected Era*. London: Springer.

TADDEO, M. (2009). Defining trust and e-trust: from old theories to new problems. In *International Journal of Technology and Human Interaction*, 5(2), 23–35.

TADDEO, M. (2010). Modelling trust in artificial agents, a first step toward the analysis of e-trust. In *Minds and Machines*, 20(2), 243–257.

TURCHIN, V. F. (1977) *The Phenomenon of Science -A cybernetic approach to human evolution* (Trans. B Frentz). New York: Columbia University Press

TWOMEY, P. (2013) Halting a Shift in the Paradigm: The Need for Bitcoin Regulation. 16 *Trinity C.L. Rev*. 67.

VERÇOSA, H. M. D. (2005). *Bancos Centrais no Direito Comparado: O Sistema Financeiro Nacional e o Banco Central do Brasil:* O regime vigente e propostas de reformulação. São Paulo: Malheiros.

WIBRAL, M. (2014), Identity Changes and the Efficiency of Reputation Systems. In *IZA Discussion Paper* n. 8216, May 2014, 1-28.

WIENER, N. (1989). *The Human Use of Human Beings: Cybernetics and Society*. Free Association Books. (original - Houghton Mifflin, 1950).

WIGDER, Z. D. *et al.* (2012) *Asia Pacific Online Retail Forecast, 2011 to 2016*: A look at Growth in Five Markets with a focus on China, Japan and Australia (July 19, 2012). Forrester Research, available online: https://www.forrester.com/Asia+Pacific+Online+Retail+Forecast+2011+To+2016/fulltext/-/E-RES72723

WILDE, O. (1891) The Soul of Man Under Socialism. In: DOWLING, L. (Ed.) *Oscar Wilde*, *The Soul of Man under Socialism and Selected Critical Prose*. Penguin Books, 2001.

YAZBEK, O. (2007) *Regulação do Mercado Financeiro e de Capitais*. Rio de Janeiro: Elsevier.