



25th IVR World Congress
LAW SCIENCE AND TECHNOLOGY
Frankfurt am Main
15–20 August 2011

Paper Series

No. 062 / 2012

Series B

Human Rights, Democracy; Internet / intellectual property, Globalization

Marco Goldoni

The Normativity of Code as Law:
Towards Input Legitimacy

URN: urn:nbn:de:hebis:30:3-249206

This paper series has been produced using texts submitted by authors until April 2012.
No responsibility is assumed for the content of abstracts.

Conference Organizers:

Professor Dr. Dr. h.c. Ulfrid Neumann,
Goethe University, Frankfurt/Main
Professor Dr. Klaus Günther, Goethe
University, Frankfurt/Main; Speaker of
the Cluster of Excellence “The Formation
of Normative Orders”
Professor Dr. Lorenz Schulz M.A., Goethe
University, Frankfurt/Main

Edited by:

Goethe University Frankfurt am Main
Department of Law
Grüneburgplatz 1
60629 Frankfurt am Main
Tel.: [+49] (0)69 - 798 34341
Fax: [+49] (0)69 - 798 34523

The Normativity of Code as Law: Towards Input Legitimacy

Abstract: In the debate on how the new information and communication technologies impact on democratic politics the role played by the digital architecture seems to be surprisingly underrated. In particular, while a lot of attention has been paid to the possibilities that new technologies open up to democratic theory, few works have attempted to look at how democracy may help in shaping technologies. By adopting as a starting point the approach known as ‘code as law’, the paper aims at two objectives: to re-affirm the importance of discussing normative principles to guide the process of code writing in order to reinvigorate the debate; to claim the importance of input reasons when deciding which principles should be chosen. After having remarked that code is relevant for establishing democratic norms, the paper briefly tackles with the main attempts by European scholars to deal with this issue. Then, a couple of practical examples of how code impacts on democratic rights are sketched out. In the last section of the paper a shift from an output-based approach to the legitimacy of code to an input-based is openly advocated: an inquiry into the legitimacy of code should focus on its production.

Keywords: Code as Law, Normative Principles, Electronic Democracy, Input Reasons

I. The Importance of Code for Democratic Politics

It is quite striking to remark, in the debate on electronic democracy, electronic government and more generally on democracy in the digital age, the relative little attention paid to the *normative* role played by the technological environment.¹ As if this aspect were taken as a given, a natural setting within which communication takes place, the role of architectural technology is rarely mentioned and explored in full depth in the research on democratic politics in the digital age.² To this assumption it must be added that electronic democracy is usually presented as an aspect of e-government, as if governmental agencies may simply digitalize political initiatives that once were only possible in the ‘physical world’.³ In this way, the setting of the technological environment is

* Research Fellow at the Centre for Law and Cosmopolitan Values, University of Antwerp. The research for this article has been generously funded by the Odysseus Programme of the FWO (Research Foundation – Flanders). I would like to thank Patricia Mindus and Andrea Greppi for having invited me to present a first draft of this article at the workshop they organized at the IVR in Frankfurt.

¹ See, for an outstanding exception, Yochai Benkler, *The Wealth of Networks*, New Haven, 2006.

² Matthew Hindman, *The Myth of Digital Democracy*, Princeton, 2009, 15-16.

³ Thierry Vedel, The Idea of Electronic Democracy: Origins, Visions, and Questions, *Parliamentary Affairs* 59 (2006), 229.

usually not contested and the debate seems to take for granted a starting point that is everything but firm and stable.⁴

On the contrary, an analysis of how democracy works in a digital environment cannot exempt itself from undertaking a critique of the architecture within which political action takes place and of the (economic, legal and social) forces that shape it. The claim here is not that nobody has looked at how digital architecture is shaped, even though this aspect has always represented a secondary interest at best. The debate has focused mainly on the contents which are passing through the digital environment and on how the Internet in particular affects democratic life.⁵ But few scholars have taken up the question of which kind of normative principles *ought* to be taken as yardstick against which judging specific codes. More precisely, it is important to look not only at how new technologies shape democratic politics, but also how democratic action can shape the same technologies. This topic becomes even more salient if one bears in mind that regulation embedded in technology, even if adopted in the most transparent way, tends to become blurred with the passing of time and no longer recognized for what it once was: a normative rule that intentionally impacts upon people's behaviour. As it will be explained below, default settings seem to have a legitimating effect because apparently the default is 'normal' to the eyes of the users.⁶

This apparent scarcity of reflection, more visible in the European debate, looks even more striking when one bears in mind that during the second half of the Nineties, a generation of cyber-scholars established the approach known as 'Code as Law' as the main point of reference. Briefly, the main contention was that contrary to the idea that the Internet is beyond the reach of regulation, as believed by the first generation of digital libertarian scholars⁷ cyberspace had begun to develop its own control mechanisms in the form of code (as distinct from traditional mechanisms tied to the State). In this context, software and hardware tend to regulate themselves. This interpretation has culminated in the bold claim that – somehow – 'code is law'. The recognition of the importance of code in regulating new technologies was mainly due to the seminal works, among others, of Lawrence Lessig⁸ and Joel Reidenberg.⁹ Faced with the problem

⁴ Scott Wright, *Electrifying Democracy?*, *Parliamentary Affairs* 59 (2006), 237.

⁵ Cass Sunstein, *Republic.com 2.0*, Princeton, 2009.

⁶ Roger Brownsword, *Code, Control and Choice: Why West Is West and East Is East*, *Legal Studies* 21 (2005) 4.

⁷ According to this perspective, the Internet is autonomous and impossible to regulate from the outside: see David Post & David Johnson, *Law and Borders – The Rise of Law in Cyberspace*, *Stanford Law Review*, 45 (1996), 1367-1402.

⁸ Lawrence Lessig, *Code and Other Laws of Cyberspace*, New York, 1999.

⁹ Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, *Texas Law*

of how to regulate cyberspace, and more generally the networks of global connection, legal scholars were convinced that the best solution could be internal and not external to the technology adopted. As a consequence of that, a dispute ensued about the real novelty brought by ICT law, and in particular by Internet law, which was well captured by the debate between the American judge Frank Easterbrook¹⁰ and Lessig,¹¹ with the reference to the so-called “Law of the Horse”.¹² In other terms, Lessig and Reidenberg, *contra* Easterbrook, remarked that the best way to cope with the problem of a powerful technology was to use the same means as a counterbalance. If code could be used to intentionally regulate human behaviour, then why not using it for good purposes? Of course, as Lessig argued, the recognition of this state of affairs posed a specific normative problem: “if code is a lawmaker, then it should embrace the values of a particular kind of lawmaking”.¹³ The idea that code is ‘really’ law is still a divisive one, and it should be noted, a growingly controversial one, up to the point where an influential commentator can remark that code is all about ‘interest group behaviour’, that is to say, code is designed as an alternative to lobbying.¹⁴ Probably, this mild but increasing skepticism on the regulatory force of code has partially hampered the flourishing of a debate on the normative criteria for assessing code as a lawmaking procedure, which still remains rather underdeveloped.¹⁵ Yet, even those who contest the idea that code is literally like law still recognize its regulatory impact, as, for example, a cautious author like Wagner does: “that technology has regulatory impact does not suggest that it is directly interchangeable with law, and it is easy to understand how the regulatory mechanisms differ”.¹⁶ This paper tries to deal with the normative implications of this regulatory power by analyzing the few works which have explored this question. In order to show the limits that a partially unaware acceptance of code as a *quasi*-natural given imposes on democratic rights, some problems concerning freedom of speech and filtering on the Internet will be outlined. The importance of introducing normative principles for regulating code does not commit to the view that “code-based change at various levels of the Internet architecture has

Review 76 (1998) 553-584.

¹⁰ Frank Easterbrook, *Cyberspace and the Law of the Horse*, *University of Chicago Legal Forum* 16 (1996), 207.

¹¹ Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, *Harvard Law Review* 113 (1999), 501-549.

¹² The dispute may be summed up in the following way: Easterbrook accused Lessig of having invented a new branch of the law out of nothing, since speaking of cyberlaw was the same as speaking of the law of the horse. Everything could be easily regulated by already existing fields of law.

¹³ Lessig (note 8) 221.

¹⁴ Timothy Wu, *When Code Isn't Law*, *Virginia Law Review* 89 (2003), 682.

¹⁵ For an exception see Egbert Dommering & Lodewijk Asscher (eds), *Coding Regulation*, the Hague, 2006.

¹⁶ Polk Wagner, *On Software Regulation*, *Southern California Law Review* 78 (2005), 458.

emerged as potentially the most powerful regulatory strategy available”.¹⁷ Nonetheless, these examples should strengthen the opportunity of reflecting on the normative criteria which should guide our judgments on code.

Finally, in the last section, given the attention paid by the relevant literature on outcome reasons, this paper argues that it is appropriate to put more emphasis on input and procedural reasons. The way code is shaped, and how users and activists can intervene on it and on the content that through it is shaped and distributed, should be seen as extremely relevant from a normative point of view. This will not make all the (ethical and legal) issues that developers and Internet users have to face quickly fade away, but it may help in re-orientating the current trend from normative arguments based on distribution to the centrality of production.

But before moving on, it is necessary to introduce a couple of clarifications. First, by code, this paper denotes software and part of the hardware that function as a set of normative rules. This normative function is common to technology understood in its widest sense, but since the focus here is on information and communication technologies, code appears to be a more accurate term.¹⁸ Moreover, following a division presented by, among others, Yochai Benkler,¹⁹ code comprises some of the layers that constitute the Internet. More specifically, he distinguishes among three layers: Content, Code, and Physical. The content layer comprises: speech, text, images, movies and every other content made available and disseminated on the Internet by its users. This content is transmitted over an infrastructure of computers and the wires that link them together. This is the physical layer. In the middle of these two layers there is the code layer. It consists of the different protocols that form its core architecture and the software upon which they run.

Second, code as law will be understood in its most inclusive way. In this context, a *lato sensu* reading of code implies to take into account the following two dimensions: on the one side, code can be a norm-enforcing technology, as it has been outlined several times in the debate; on the other side, code can be also a norm-establishing technology as well. The recognition of these two aspects of code makes a reflection on normative principles extremely relevant.

¹⁷ Stephan Biegel, *Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*, Boston, 2001, 362.

¹⁸ To avoid too many repetitions, I will use ‘architectural regulation’ as a synonym of code as law.

¹⁹ Yochai Benkler, From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access, *Federal Comm. Law Journal* 52 (2000) 562-563.

II. Code and Rules

For a legal theorist, one of the most interesting aspects of code is the intentional feature of its regulatory impact. This makes it somehow close to certain features of the law as understood in the classic positivist tradition from Austin to Kelsen, even though code cannot be equated to a command backed with sanction. Nonetheless, architectural regulation raises normative issues because of some of its operational aspects. We should not forget that code sets certain features which represent the framework within which action takes place: most importantly, they are features selected by code writers; they constrain some behaviour (for example, electronic eavesdropping) by making other behavior possible (for example, encryption). They embed certain values, or on the other side they exclude them.²⁰ Under certain aspects, code works as constitutive rules do.²¹

Besides, code is being used more and more as law for regulating human behaviour. Both Lessig and Reidenberg have provided examples of how rules are embedded in code. Reidenberg, in particular, made it clear that choice of design in systems impose rules on participants: the creation and implementation of information policy are embedded in network designs and standards as well as in system configurations. Traditional rule-making appears to be extremely different from architectural regulation: “in the context of information flows on networks, the technical solutions begin to illustrate that network technology itself imposes rules for the access to and use of information”.²² Other authors have stated clearly in which sense code is made of rules:

in terms of optimal lawmaking analysis, technological standards are closely related to legal rules. For example, both substantive rules and technological standards influence user behaviour directly. As technological standards’ influence on behaviour increases, they will increase in similarity to legal rules. Rules are best promulgated by centralized institutions, particularly public, governmental institutions ... Moreover, the task of formal political institutions should be to confirm the legitimacy of choices made by de facto standard setters by ensuring that all interested parties are involved and by exercising an appropriate control structure over decentralized standard setting.²³

To cut a long story short, code as law is normative in the sense that it regulates and guides human behaviour. This is the specific aspect of code as law with which this paper deals.

²⁰ Lessig (note 8) 202.

²¹ See John Searle, *The Construction of Social Reality*, New York, 1995.

²² Reidenberg (note 9) 568.

²³ Daniel Benoliel, Technological Standards, INC: Rethinking Cyberspace Regulatory Epistemology, *California Law Review* 92 (2004), 1116.

As reminded by Ludwig Asscher,²⁴ there are several cases where code is used for self-regulation. First, code is used to enable the enforcement of rights. Code is a potentially perfect tool of enforcement. If technology completely prevents one from copying a book, a copyright infringement becomes very difficult. Second, if technology blocks the access to certain prohibited information, the distribution of that information has been stopped much more efficiently than if a judge would have declared that piece of information to be unlawful. Code can also be used as a tool for self-regulation. Architectural regulation shapes the relationship between private parties with no need for government to step in. Finally, code may in different ways be replacing the traditional balancing of interests: if code is replacing the role of a judge when considering limitations to a particular right, then it is replacing the enforcement of that right.

A key difference between code and law, however, pertains to the kind of rules that belong to these two regulative tools. To take into account this difference may caution against an enthusiastic embrace of this modality of regulation because while legal norms determine how people *should* behave, leaving them the possibility to choose whether to comply or not, code, particularly in its norm-establishing version, determines how people *can* behave. By remarking that code is an efficient means of regulation, Lessig also noted that its perfection can make it into something more controversial: “One obeys these laws as code not because one should; one obeys these laws as code because one can do nothing else. There is no choice about whether to yield to the demand for a password: one complies if one wants to enter the system”.²⁵ In a nutshell: Compared to legal norms, code can become a much more pervasive, yet not always visible, mean of control. The case of privacy is quite telling of how code has already upset the traditional regulatory balance by threatening the protection of this value beyond the control of courts and parliaments.²⁶

Often the very features of code that make it a viable (and attractive) alternative to legal regulation can have troubling effects, at least as compared to legal regulation. From a democratic point of view, the public dimension of lawmaking is deemed to be valuable and necessary. In a recent essay, Jeremy Waldron has proposed an attractive definition of this aspect of lawmaking in terms of “the way law presents itself as a body of rules dealing with matters that are appropriately

²⁴ Lodewijk Asscher, ‘Code’ as Law. Using Fuller to Assess Code Rules, in: Dommering & Asscher (note 15), 70.

²⁵ Lawrence Lessig, The Zone of Cyberspace, *Stanford Law Review* 48 (1996), 1408.

²⁶ Cf Bert-Jaap Koops & Ronald Leenes, Code and the Slow Erosion of Privacy, *Michigan Telecommunication & Technology Law Review* 12 (2005), 115-188.

matters of public concern and dealing with them in a way that can stand in the name of public”.²⁷ If the public aspect of lawmaking is recognised and taken into account, then the role of code writing needs to be put under a different light. Of course, one may object that legal rules not always are clear and that lawmaking procedures often take place behind curtains, in the realm of lobbying and interest bargaining. However, most of the times, the outcome is public and visible, and even though not all citizens may be aware of the existence of a legal rule, they may easily retrieve it.²⁸ Rules also need some minimal level of enforcement and this is normally a human and complex activity. Non-compliance with rules, in order to be meaningful, must be detectable by the appropriate agency. The actors involved in this operation usually possess discretion and exercise judgment on their reasons for action. This is part and parcel of the social organization of the law and public processes of enforcement are instrumental to it.²⁹

Code functions in another way. As famously argued by Walter Benjamin about the fruition of architecture (for whom buildings are appropriated in a twofold manner: “by use and by perception”),³⁰ people simply find themselves in an architectural environment. The element of consent or choice tends to disappear within code. One cannot often say that one chooses to obey to the rules of code. One of the most recurrent discussions in legal theory is about the question of whether there is or ought to be an obligation to obey the law, and which kind of aspect of the law (its content or its sources) makes legitimate its authority.³¹ In fact, code may not leave any possibility of choice. Once entered into the architecture, an agent cannot choose whether to obey a rule or not. Besides, code can provide for perfect enforcement, leaving no room for breaking (or disobeying) a normative rule. Finally, rules established by code have often a blurred pedigree and from the enforcement perspective, architectural regulation bypasses many of the possibilities for human actors to modulate the effects or meaning of a rule in the enforcement process, which is, instead, delegated to technological settings. To these considerations, it must be added that even the rules and the institutions which govern the Internet are not immune from the same kind of criticism. For example, the development of Internet Corporation for Assigned Names and Numbers (ICANN) has been subject to severe criticism, both of its institutional design and its

²⁷ Jeremy Waldron, *Can There Be a Democratic Jurisprudence?*, *Emory Law Journal* 58 (2009), 700.

²⁸ Lee Tien, *Architectural Regulation and the Evolution of Social norms*, *Yale Journal of Law and Technology* 4 (2003), 8-10.

²⁹ *Ibid.* 10.

³⁰ Quoted by Neil Katyal, *Architecture as Crime Control*, *Yale Law Journal* 111 (2002), 1072.

³¹ For opposite takes on this issue see Joseph Raz, *The Authority of Law* (1979), Oxford, 2009; John Finnis, *Natural Law and Natural Rights* (1980), Oxford, 2011.

actual workings.³² These considerations stress the lack of any public process over norm-establishing and norm-enforcing through code. These controversial aspects also remind of the need of looking for normative criteria for assessing code as law.

Even though these features of code as lawmaker are recognized by scholars, a certain initial enthusiasm was common among many of them for what concerns the capacity of code to shape the environment. Digital libertarians, in particular, firmly believed in the impossibility and undesirability of traditional law to shape code. This initial interest in the emancipatory force of code seems to have left the place to a more alarming and critical analysis. Once certain problematic features of code are taken into account, the demands for normative principles cannot be eluded any longer.

III. The Narrative of Code as Law: From a Descriptive to a Normative Approach

With the exception of those who did not believe the Internet would represent anything substantially new, a lot has been written about the liberating virtues of code as law, in particular against a formal legal positivist approach and a State-based understanding of the sources of law. Legal pluralists, for example, have seen in the raise of code an enriching factor for the legal world and an increase in freedom.³³ Bypassing the State as the centralized machine for lawmaking looked as a great chance to consolidate and augment individual freedom to their eyes. Yet, in the last ten years a growing skepticism can be detected and this represents another important factor in favour of adopting normative criteria.

As noted, the first pioneering cyberlaw authors did not pay too much attention to the normative dimension of code. According to Lessig, the most prominent among these authors, regulating new technologies is a difficult task, which demands to look at a multiplicity of modalities. For him, the key is to balance among the different types of regulatory modes. Which are these potential regulatory modes? Lessig lists four:³⁴ the law, the market, social norms and the architecture (or code). There is no regulation in general, but only specific modes of regulation and each constrains differently: the legal, the economic, the social and the technological modes, which are respectively denominated as law, norms, market, and architecture. For Lessig, regulating new technologies implies a right and balanced mix among these four factors. This is

³² See the devastating critique of Milton Mueller, *Ruling the Root. Internet Governance and the Taming of Cyberspace*, Cambridge Mass, 2002; cf Michael Froomkin, Habermas@discourse.net: Toward a Critical theory of Cyberspace, *Harvard Law Review* 116 (2003), 751-872.

³³ Paul Schiff Berman, Global Legal Pluralism, *Southern California Law Review* 80 (2007), 1155-1237.

³⁴ Lessig (note 8), 235-239.

what Lessig calls “the optimal mix”. A good illustrative example of how a mix may work is provided by Lessig himself by explaining the regulation of seat belts:

The government may want citizens to wear seatbelts more often. It could pass a law to require the wearing of seatbelts (law regulating behavior directly). Or it could fund public education campaigns to create a stigma against those who do not wear seatbelts (law regulating social norms as a means to regulating behaviours). Or it could subsidize insurance companies to offer reduced rates to seatbelt wearers (law regulating the market as a way of regulating behaviour). Finally, the law could mandate automatic seatbelts, or ignition-locking systems (changing the code of the automobile as a means of regulating belting behaviour). Each action might be said to have some effect on seatbelt use: each has some cost. The question for the government is how to get the most seatbelt use of the least cost.³⁵

Overall, the optimality requirement depends and varies according to its object.

Lessig’s suggestion is “that we have to understand how the different modalities regulate and how they are subject, in an important sense, to law, then we will see how liberty is constructed not simply through the limits we place on law. Rather, liberty is constructed by structures that preserve a space for individual choice, however that choice may be constrained”.³⁶ From this point of view, law becomes a meta-regulator, which means, in this case, that it adjudicates how other regulatory means have to be employed.

Yet, Lessig does not treat the question of which normative principles should guide the regulatory activity, with the exception of some passages and a reference to the importance of individual choice, here understood as the possibility of leaving open certain options in the digital architecture to the user. This lack of reflection comes at a price. In fact, as Lessig himself points out, indirect control can be used astutely by the government, and one must add, also by private actors. The example of access to the public beaches on Long Island is a good one. If regulators declare openly and directly that African Americans are not allowed to use the beaches, the regulatory position and its objectives are perfectly visible and transparent. If, instead, regulators pursue the same objective indirectly by constructing narrow bridges or the like, then it might be much less clear what is going on and it would become more difficult to have a public debate (and possibly a conflict) on the issue.³⁷

Joel Reidenberg’s move from a descriptive to a more critical stance towards code is quite indicative of a change of perspective in the literature on code as law. In his influential article on ‘Lex Informatica’ (shaped after the *Lex Mercatoria*), he did take a neutral stance toward the

³⁵ Ibid., 93-94.

³⁶ Ibid., 345.

³⁷ Lessig (note 11), 541-543.

possible conflict between institutional law and code as law (*lex informatica*, indeed). He simply remarked how *lex informatica* could provide several effective tools for legal regulation. He, like Lessig, has not systematically articulated criteria for the acceptability of *lex informatica*, but some of them can be inferred from his work. In fact, during the last decade, Reidenberg has moved toward an increasingly cautious perspective on *lex informatica* and he has started to advocate a more active role for traditional law. For this reason, he tends to stress the importance of political control: “because technical designs and choices are made by technologists, government policymakers should play an important role as public policy advocates promoting policy objectives”.³⁸ Reidenberg provides two criteria that should guide the regulation of code: legal authority and proportionality. For what concerns the first, “as a threshold matter, states must have a legal process in place to authorize the use and choice of technological enforcement tools’, while for the second, he believes that ‘the basic principle ... should be that a state only use the least intrusive means to accomplish the rule enforcement’”.³⁹ In the balance, the second principle seems to give to *lex informatica* a major role in the realm of regulation.

While many American scholars seemed to have identified in the emergence of code a huge potential for more freedom and creativity,⁴⁰ Europeans have adopted from the very beginning a much more cautious approach. Here, we will mention three European authors – to our knowledge, the only ones⁴¹ – who have tried to propose normative criteria for evaluating code as law.

The first one is also the most cautious. Roger Brownsword, in his discussion of ‘techno-regulation’ (his term for architectural regulation) accepts Lessig’s classification of the regulatory modalities, but believes that there is an unavoidable conflict between the modalities coming from the law and the society (East Coast code) and the technological forces of code (what he calls West Coast code) because of the pressure coming from the latter to self-regulate themselves. By

³⁸ Reidenberg (note 9), 580.

³⁹ Joel Reidenberg, States and Internet Enforcement, *University of Ottawa Law & Technology Journal* 1 (2004), 229.

⁴⁰ This attitude has been aptly summed up by James Boyle, Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors, *University of Cincinnati Law Review* 66 (1997), 205: “The attraction of technical solutions is that they apparently elide the question of power – both private and public – in the first place. The technology appears to be ‘just the way things are’; its origins are concealed [...] Above all, technical solutions are less contentious; we think of a legal regime as coercing, and a technological regime as merely shaping [...] our choices”.

⁴¹ It is worth mentioning the work of Luciano Floridi on information ethics, even though his proposal is based on philosophy of information and does not put moral agency at its centre. Therefore, his moral principles concern mainly entropy: “entropy ought not to be caused in the infosphere (null law); 1) Entropy ought to be prevented in the infosphere; 2) Entropy ought to be removed from the infosphere; 3) Information welfare ought to be promoted by extending (information quantity), improving (information quality), and enriching (information variety) the infosphere”: Luciano Floridi, Information Ethics: On the Philosophical Foundation of Computer Ethics, *Ethics and Information Technology* 1 (1999), 47.

presenting the issue in this way, Brownsword has already paved the way to the primacy of institutional law. He basically proposes two criteria for regulatory intervention: effectiveness and legitimacy. The latter seems to be equal to respect of human rights and human dignity. More precisely, he seems to regard human rights and human dignity as co-essential. Or, to put it in a concise way, he considers human dignity as empowerment (as opposed to dignity as a constraint) to be realized through human rights. A critical consequence of this view of the centrality of human rights is that human beings should have a choice: the autonomy that underpins human rights “implies the provision of a context offering more rather than fewer options”.⁴² The point of Brownsword’s critique of code as law lies here: it is constitutive of human dignity not only that right choices are made, but also that wrong choices can be made. As a result, Brownsword’s key criterion for assessing compliance-proof architectural regulation is freedom of choice.⁴³

Bert-Jaap Koops has produced one of the most articulated lists of normative criteria, at least compared to other attempts at formulating criteria for architectural regulation. He distinguishes between primary and secondary criteria and establishes a hierarchy between them. Primary criteria are mostly substantial and they include human rights (clearly the most important factor in his view), other moral values that a society considers relevant (e.g., autonomy, dignity), and some procedural values, like democratic decision-making and inclusive participation. Secondary criteria include transparency, accountability, and output criteria of the likes of efficiency, flexibility, context-adaptability.⁴⁴ To sum up Koops’ position, primary criteria should be met before the secondary criteria come into view. Among primary criteria, substantial ones shall prevail over procedural ones. Of course, given the rather abstract and broad criteria advanced by Koops, assessments cannot yield a categorical answer of the kind yes or no, but only a degree-based answer of the kind ‘more-or-less’. Be that as it may, the hierarchical order does provide a bottom-line: if core principles are met only to a low extent, then the overall assessment must be negative. In the balance, Koops seem to believe that what counts as primary is the output of code writing. As is the case for Brownsword, Koops adopts a primarily output-oriented approach, where the respect of human rights becomes the key parameter of evaluation. The difference is that according to Koops the scope of the technology in question and of its jurisdiction are also key elements to be taken into account for assessing the acceptability (this is the word that he

⁴² Roger Brownsword, *What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity*, in: *Human Rights*, ed. R. Brownsword, 2004, 218.

⁴³ *Ibid.*, 230-231.

⁴⁴ Bert-Jaap Koops, *Criteria for Normative Technology*, in: *Regulating Technologies*, ed. R. Brownsword, 2008, 159.

employs) of a code. If one does not know what the scope of a particular technology is, it is not possible to establish whether the application of that same technology is acceptable in a particular jurisdiction.

Finally, another systematic attempt to offer a set of criteria to assess code has been made by Lodewijk Asscher. After having established that the rules embedded in code cannot be compared to legal rules, he discards positivism as an inapt normative legal theory for code as law and he suggests turning the attention to Lon Fuller's criteria for the legitimacy of law (and to the criteria for freedom of expression sketched out by the European Court of Human Rights). This move leads to a series of questions that, according to him, should guide any assessment of code as law: "1. Can rules be distinguished in the code? 2. Are these rules accessible to the public? 3. Can these rules be reliable, in the sense that they are predictable? 4. Is there an authority that makes the code rules? 5. Is there a choice? Can the citizen choose not to obey the rules? Can they choose another system of code?"⁴⁵ Once again, here we see a mix of input (question number 4) and output criteria, but even though the reference to Fuller's inner morality may bring to think at a primarily output-based approach, Asscher reminds us of the importance of democratizing some of the most crucial code writing.⁴⁶ This is indeed one of the few remarks in the literature whose attention goes to the *normative* relevance of the production of code. But before proceeding further into this aspect of the legitimacy of code as law, it is necessary to take a brief detour in order to show how particular kinds of code-writing processes impact on certain democratic rights.

IV. Two Examples: Freedom of Speech and Filtering

Freedom of information and freedom of speech are fundamental rights for any theory of democracy. And it is undeniable that architectural regulation influences the flow of information in society. Control of content can be achieved through the regulation of any of the three layers we made reference to in the first section. As remarked by Larry Solum and Chung, efforts to control speech are often realized through regulation in the lower layers of the network system (Code and physical layers, more than content). A discrepancy occurs between the places where targeted speech is conducted and where it is countered. As control is taken from the ends and moved into the architecture, a conflict arises with the notorious end-to-end argument and the principle of

⁴⁵ Asscher (note 24), 85.

⁴⁶ *Ibid.*, 88.

layer separation.⁴⁷ Regulation of content at the physical layer can lead to a conspicuous blockade of speech (geographically bounded); regulation at the code network layer may block speech from a certain host machine (IP filtering); regulation at the code application layer (URL filtering) is limited to the speech contained in a certain document.⁴⁸ Regulation (and control) of information can take place both at the ends of the network or at its *ins* (source and destination ISPs). Information control by service providers may prove to be more feasible than going after a wide variety of individual users. The provider is a node in the Internet chain where the enforcement of law and code regulation can be facilitated in a relative easy way. An ISP may function as a link between the user and the Internet, that is, as a vehicle for packets of data. An ISP may also host its own or other people's content on its server. In both cases, it is possible to limit the flow of information through institutional law (think, for example, at the liability regime) and, crucially for the topic of this paper, through code.⁴⁹

Another relevant example of the importance of code for freedom of information that is exercised at the users' end level is represented by the case of filtering. Control of information from the side of the data flow has been mainly achieved by filtering technologies. This is a technique which may also deeply affect freedom of speech, yet the way it is put into practice through the regulation of the Internet puts certain values of good governance like legitimacy and accountability at risk, without letting users to be aware of how and when they are controlled. Geolocation techniques offer geographic localization by connecting IP addresses to the nationality of a user. This kind of technology facilitates, for example, the adjustment of language per region. But it also supports more personal advertising and the enforcement of local law. The blocking of region specific IP addresses at the network layer could prevent the access to sources.⁵⁰ Efforts at streaming the information flow on the basis of localities have not been limited to lawsuits. Google's search engine represents the most known example of a practice of filtering based on a more informal approach. For example, in March 2001 Google removed the

⁴⁷ Lawrence Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law*, *University of San Diego School of Law Research Papers*, 2003, 26-27.

⁴⁸ *Ibid.*, 65.

⁴⁹ Zittrain notes that the destination ISP has the obvious advantage to be a node located inside the jurisdiction of the state that seeks to regulate certain information or speech. By coining the case of the Pennsylvania Model, Zittrain underlines the importance of the last node in the transmission chain, which provides probably the most effective point of blockage for information flowing from foreign soil. China and Saudi Arabia use the backbone ISPs for countrywide filtering of incoming flow of data: Jonathan Zittrain, *Internet Points of Control*, *Boston College Law Review* 43 (2003), 655-658.

⁵⁰ An (in)famous case in which this technique was claimed to implement a judicial decision is the *Yahoo!* Case.

links to web pages that contained material that allegedly infringed the copyright of the church of Scientology.⁵¹

As regards legitimacy, the use of technology to exert control over Internet users frequently challenges tenets associated with the rule of law, concerning both the process for (and content of) norms governing behaviour. These challenges emerge, in particular, where technology is linked to compliance with voluntary codes or soft law instruments by non-state actors. Whilst it may be suggested that the voluntary character of compliance with such instruments reduces or removes the requirements suggested by the rule of law, the consequences of compliance will often accrue to third parties who do not experience compliance as voluntary and in situations where many of the elements of the regime of control are determined by non-state actors outside of the normal public policy process. The combination of automatic enforcement, opaque systems and rules directed at intermediaries may leave affected users unaware that their behaviour is being controlled, so that the opaque nature of filtering may result in a loss of accountability. Where it is not clear what is being blocked, why, or by whom, the operation of mechanisms of accountability – for example: judicial review – is greatly reduced.

V. Input Criteria for Legitimacy

It is time to take stock and, in light of the previous considerations, to take up the question of the normative criteria to be applied in order to assess the legitimacy of code as law. This is done with the aim of reinvigorating a debate on this critical topic.

As a framework for evaluating the legitimacy of code one can refer to the distinction between input and output reasons.⁵² Input reasons are those reasons that apply to the procedural aspects of decisions, that is, to how a decision is reached. As a measure for legitimacy, input reasons take into account the fairness of the adopted procedure. Output reasons concern the content of decisions and they represent a moral yardstick for judging the legitimacy of technologies. What counts as legitimate, according to the output-based perspective, is the end result of a decision and its normative content, not how the decision was reached.

Those who have tried to put forward normative criteria for assessing code as law have mainly put the accent on output reasons, with human rights obviously playing a major role. As

⁵¹ The case is discussed in Benjamin Edelman & Jonathan Zittrain, *Internet Filtering in China*, 2003, available at <http://cyber.law.harvard.edu/filtering>.

⁵² The classic references for this distinction are Fritz Scharpf, *Governing in Europe*, Oxford, 1999; Jeremy Waldron, *The Core of the Case Against Judicial Review*, 115 *Yale Law Journal* (2006) 1396-441; Richard Bellamy, *Political Constitutionalism*, Cambridge, 2007.

noted above, Brownsword has stressed the importance of respecting human rights and human dignity for judging the legitimacy of code as law.⁵³ Koops has affirmed that the best methodology for the acceptability of what he calls ‘normative technology’, “does not lay [in] procedural justice, in which the criteria would be valid because the right procedure was followed to find them, but rather to *outcome justice*, in which the criteria are valid because the outcome is accepted by the reader as a reasonable one”.⁵⁴ In a rather typical legalistic and formalist fashion, Koops would also have lawyers testing the set of criteria for normative technology. This sounds as a call for a debate among specialists, in order to build a firmer and more accurate set of criteria. If one takes for granted that lawyers are bearers of a culture of respect for human rights, and in particular for the right to privacy and freedom of speech, then the active involvement of the legal community may make the writing of code more sensitive to these values. Nonetheless, it is far from clear whether this is more than a necessary (but not sufficient) condition to have fair normative criteria respected in the production of code.

Given the nature and the logic of architectural regulation, the emphasis on output legitimacy is misplaced for several reasons. First, since technology is often irreversible – once it is developed and applied in society, it is difficult to change it or remove it from society in those applications – the process which develops code as law becomes a key concern when normativity is at stake. In fact, it may well be too late when a particular version of a technology appears or is adopted in a given society to ask whether it is acceptable to keep a certain technology. The difficulty of reversing embedded code is often evident and makes it fundamental to focus on the procedure and the actors involved in the development of the technology. Second, given the opacity of architectural regulation, to be aware of how technology is directly or indirectly impacting upon agents’ behaviours may prove to be too difficult in many cases. Last but not least, as mentioned in the first section, the importance of default technology cannot be underestimated. What appears to be default code is often taken as a natural and immutable fact. Of course, default settings entail choice. Nonetheless, the regulatory target of code need not be aware that there has been a decision to constrain or control his actions. On top of that, it is known that users often follow default settings even when they are against their best interest. This is usually explained by making reference to two factors. People do not change defaults because they are uninformed. A default setting is essentially useless if a person does not know about the

⁵³ Brownsword (note 42), 210.

⁵⁴ Koops (note 44), 167.

possibility of changing the option or the ramification of each choice.⁵⁵ The second reason why people do not change their setting defaults is because of their lack of technical knowledge. If people cannot figure out how to change settings, they cannot modify it by definition.⁵⁶

For these reasons, input-based legitimacy should become the primary concern in choosing normative criteria. But which kind of input reasons is to be placed at the center of the evaluation of the design process? Given that code is not exactly like law, it is difficult in the realm of code to adopt a kind of rule of law (or ‘rule of code’) approach. Yet, we have also seen that when a particular code is ‘enacted’, it may be too late to remedy to the violation of certain rights. This is why the accent should be put on the moment of production, rather than on the moment of distribution. The moment of production should be assessed according to two intertwined principles: one is transparency and publicness. Decisions, in order to be accountable, should be known and also the procedure that brought to that decision should be disclosed. The second principle that should guide the ‘writing’ of code is equal chance of participation to the process, which also entails the idea that the writing process should be as inclusive as possible.

The predictable example of an inclusive and egalitarian participation in the definition of code is the case of F/OSS (Free/Open Source Software) communities, which are considered important agents of democratic participation. Clearly, F/OSS communities should not be romanticized, otherwise one runs the risk of falling into the trap of technological utopianism. For example, the issues of ‘forking’ and the disagreement between free software advocates and open source developers remind us that the F/OSS communities are everything but a monolithic universe.⁵⁷ But the study of these communities reveals that issues of democratic production of code are still central and when approached in an inclusive and open way, it turns out to be also the most fruitful one.⁵⁸ At this stage, the argument advanced by Jack Balkin in support of a democratic digital culture should clearly resonate here:

a ‘democratic’ culture ... means much more than democracy as a form of self-governance. It means democracy as a form of social life in which unjust barriers of rank and privilege are dissolved, and in which ordinary people gain a greater say over the institutions and practices that shape them and their futures. What makes a culture democratic, then, is not democratic governance, but democratic participation.⁵⁹

⁵⁵ Rajiv Shah & Jay Kesan, Manipulating the Governance Characteristics of Code, *Info* 5 (2003), 7.

⁵⁶ Cass Sunstein, Switching the Default Rule, *N.Y.U.L. Review* 77 (2002), 106-134.

⁵⁷ Michael Dizon, Free and Open Source Software Communities, Democracy and ICT Law and Policy, *International Journal of Law and Information Technology* 18 (2010), 127.

⁵⁸ *Ibid.*, 141.

⁵⁹ Jack Balkin, Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information

It is time to shift again the discourse from distribution to production and focus on how the digital environment is created. The closest analogy to what is proposed in this paper is to the way commons can be governed,⁶⁰ in terms of non-hierarchical participation to its production and preservation.⁶¹

Finally, two cautionary notes concerning the assessment methodology are in order. First, there is always a gap between a norm promulgated by the legitimate public authority and its translation into a technology. In other words, there is always a difference between ‘law in books’ and ‘law in technology’.⁶² In the translation process, choices and reductions take place, and these may not be necessarily made in the most inclusive way by technology developers. Second, the scope of normative criteria cannot be constrained to public institutions. These criteria should also become relevant for technology that is developed where private parties build in norms in order to influence users’ behaviour. Code is not only the *longa manus* of official law, but can also be an instrument of power of the market or of civil society.⁶³ In light of the emergence during the last decades of de-regulation as a landmark of policy in the private sphere, it is even more urgent to extend the normative criteria (and possibly constitutional safeguards) to the private development of architectural regulation. Moreover, the growth of polycentric governance, where multiple layers of supranational, national and local institutions are combined with non state-actors regulation, makes any sharp distinction between public and private regulation hard to maintain. One can think at cases where the relevance of private regulation is manifest, like, for example, a case of a search engine filtering information that concerns the same company that runs the search engine, or worse, information that shed a bad light on the political forces which are supported by this company. Nonetheless, not every private regulation has to be subjected to the same scrutiny: it will depend on the context.

This last remark brings us to a final consideration. It is quite hard to judge architectural regulation from a general and purely universal perspective. To evaluate the acceptability of architectural regulation as such is extremely complex and it seems not to take into account the

Society, *N.Y.U.L. Review* 79 (2004), 33. The gist of Balkin’s argument is that, in the digital age, the focus of democratic theory and practice should be on participation rather than governance.

⁶⁰ Eleanor Ostrom, *Governing the Commons*, Cambridge, 1990.

⁶¹ This does not commit to the view that the Internet as a network is in itself a commons. The contextual approach here advocated would prefer to treat the Internet as a composite good, a mixture of public goods, common pool resources and private goods: Cf Justyna Hofmokol, The Internet Commons: Towards an Eclectic Theoretical Framework, *International Journal of the Commons* 4 (2010), 226-250.

⁶² Mireille Hildebrandt & Bert-Jaap Koops, A Vision of Ambient Law, *Fidis* (deliverable), 2007, 22 (available at www.fidis.net/fidis-del).

⁶³ Dommering & Asscher (note 15), 249-255.

great variety in codes that nowadays has become apparent. Furthermore, the assessment of code may vary according to the modification of the technology itself, which impacts upon the interpretation of the criteria overtime. Code may go through several stages and judgments on its legitimacy passed at a certain time may differ radically from the conclusions drawn previously at a later moment. This means, in other words, that it is not promising (actually, it may look Sisyphean) to ask in abstract whether a privacy-friendly identity-management system is a good code. It is also important to determine what are the persons most affected by the code and to establish who might have a say in the design process, which means, moreover, that normative criteria are necessary also in order to identify the relevant groups. Therefore, it is unavoidable to focus on the specific code one wants to assess and to address the affected communities. Context-sensitivity is essential in this case; the application of the normative criteria outlined above implies the interpretation and the weighing of the input-based principles in the concrete instance. This is a challenge and an invitation to develop further and in a more detailed way the normative criteria we want to adopt for a more inclusive and transparent architectural regulation.

The necessity of dealing with this question will become even more urgent because of the emergence of new technologies. As aptly remarked by Mireille Hildebrandt and Bert-Jaap Kooops,⁶⁴ ambient-intelligence technologies will represent another challenge for the discourse on the legitimacy of ICT media. Ambient intelligence is a kind of technology made of smart environments that continuously make instantaneous decisions on citizens and consumers based on profiles and large collection of personal data. In such an environment, legal norms for the protection and enhancement of the privacy and equality of citizens will be inadequate. ‘Ambient law’ will be embedded in the ambient intelligence structure and this will pose other serious problems of legitimacy. In particular, choice as a normative principle will be put into question as this kind of technology changes its offers as a reaction to the person with which is communicating. And this represents another strong reason to focus primarily on the production of code rather than on its outputs.

⁶⁴ Mireille Hildebrandt & Bert-Jaap Kooops, The Challenges of Ambient Law and the Legal Protection in the Profiling Era, *Modern Law Review* 73 (2010), 428-460.

Address:
Marco Goldoni
Faculteit Rechten
Venusstraat 23
University of Antwerp
Belgium
marco.goldoni@gmail.com