

Norms, Laws and the Internet

Enrico Pattaro
Giovanni Sartor

September 23, 2002

1 Introduction

This presentation will start with an obvious statement and move into a controversial one.

The obvious statement is that the Internet is a global phenomenon.

First of all, the Internet global since it concerns a significant, and increasing, share of the world's population.¹

Secondly, the Internet is global in regard to the geographical distribution of its users, who inhabit every country of the world (though enormous diversities in the penetration rates in different countries).²

Thirdly, the Internet is a global phenomenon since its distributed architecture allows in principle everyone of its nodes (and therefore every part of the world) to be both a provider and a user of global information.³

Fourthly, the Internet is global being one of the main causes of globalisation. Thanks to the Internet physical distance becomes irrelevant to communication, a global space is realised where personal interactions and organisational structures may be distributed all over the world, regardless of physical proximity.⁴

Fifthly, the Internet is a global phenomenon in the sense that it involves every sector of human activity. Not only in cyberspace we reproduce those activities that we used to perform in physical space, but the Internet is modifying the way in which all activities are carried out, from scientific research, to production, to

¹As Castells ([7], 3) reports: At the end of 1995, the first year of widespread use of the world wide web, there were about 16 million users of computer communication networks in the world. In early 2001 there were over 400 million; reliable forecasts point to about 1 billion users in 2005, and we could be approaching the 2 billion mark by 2010.

²For a synthetic account of the geography of the Internet, cf. Castells ([7], 207 ff.)

³For an account of the formation and the basic features of the architecture of the Internet, cf. Naughton ([17]).

⁴For the statement that communication technologies are the main factor of globalisation, and the Internet the "most profoundly important of them", cf., among others, Hutton and Giddens ([12], 1). For a discussion of how the Internet provides the infrastructure for a global social space, substituting a "space of fluxes" to the "space of places", cf. Castells ([6], 407 ff.). On proximity factors, and how the Internet modifies them, cf. also, for example, Axelrod and Cohen ([3], 68 ff.).

socialisation. Cyberspace merges with physical space, providing the substrate for a new type of social organisation.⁵

The controversial statement concerns the fact that the Internet needs a legal regulation. As we shall see in the following, attempts to use law to govern the Internet have been questioned in the past. There have been critiques concerning the feasibility of those attempts, but there have been also critiques concerning their opportunity and legitimacy. Here is how one of the libertarian prophets of the Internet, John Perry Barlow ([4]), co-founder of the Electronic Frontier Foundation, and lyricist of the Grateful Dead rock band, views the encroachment of the law over the Internet, in his famous declaration of independence of cyberspace.⁶

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather. We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear. Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions. You have not engaged in our great and gathering conversation, nor did you create the wealth of our marketplaces. You do not know our culture, our ethics, or the unwritten codes that already provide our society more order than could be obtained by any of your impositions. You claim there are problems among us that you need to solve. You use this claim as an excuse to invade our precincts. Many of these

⁵Here is how Castells ([6], 5), characterises this aspect of the Internet “If e-business is understood as the commercialization of the Internet by dot.com firms, this would be an interesting, innovative, and sometimes profitable business, but rather limited in its overall economic impact. If, as I shall argue, the new economy is based on unprecedented potential for productivity growth as a result of the uses of the Internet by all kinds of business in all kinds of operation, then we are entering, probably, a new business world. A word that does not cancel business cycles or supersede economic laws, but transforms their modalities and their consequences, while adding new rules to the game (such as increasing returns and network effects).”

⁶Barlow was one of the leaders of the protest against the US Communication Decency Act, the law made it a federal crime to send obscene or indecent messages over the Internet to anyone under the age of 18 or to post sexually explicit material that could be viewed by anyone under 18. That law was then struck down by the US Constitutional Court in 1997 (the U.S. Supreme Court as overly broad and in violation of the First Amendment (freedom of speech)).

problems don't exist. Where there are real conflicts, where there are wrongs, we will identify them and address them by our means. We are forming our own Social Contract. This governance will arise according to the conditions of our world, not yours. Our world is different.

The libertarian worries expressed by Barlow have been contrasted by a number of requests apparently going in the opposite direction, i.e. pleading for the legal governance of the Internet. There have been voices coming from governments, which are interested in controlling the net for policing purposes (preventing crimes and especially terrorism), for censoring certain types of information (such as pornography, paedophilia, hate speech, nazi propaganda, etc.), for controlling dissent. Other, stronger and more successful voices, have come from the business community, requesting a legal framework for electronic commerce, a judicial protection of domain names, and a strong defence of intellectual property. Finally, voices motivated by civil right concerns have been advocating legal protection for on-line privacy, preservation of the fair use of cultural products (the preservation of cultural commons), and more generally the warranty that the law ensures that Internet remains an environment where civil, social and cultural rights can be safely exercised.

So, on the one hand the Internet seems to refuse law and politics, as antiquated impediments to its creativity, as authoritarian obstacles to new and better forms of (self-)governance; on the other hand it asks for legal solutions (and different voices are often asking for very different legal solutions) for the new "political" problems brought about by this very creativity, problems for which a shared and consented outcomes, voluntarily adopted and even implemented by everybody within the Internet community, seems to be out of reach.

The starting point for our discussion will be an attempt to establish what the law is, in regard to other possible ways of regulating the Internet. Then we will consider the role of the law in governing the Internet in a diachronic perspective. Finally, we will try to reach some tentative forecasts and normative conclusions.

2 The law

Let us start our discussion of the law by analysing another libertarian statement coming from the Internet community. Peter Ludlow ([16]) says:

Governments and governmental institutions and laws *have* a kind of reality, but it is pretty clearly a socially constructed reality. I would even go so far as to say that it is a kind of consensual hallucination. Consider the Los Angeles Police Department. It has a certain authority in Los Angeles, but I would argue that it has this authority only by virtue of a consensual hallucination that the denizens of L.A. have bought into. Some might argue that it has its authority by virtue of the guns it carries, but this is pretty clearly false. The LAPD can handle the odd drunk driver or jewel thief, but

tomorrow if even 1% of the population decided to ignore the laws of Los Angeles the police would be helpless

From this idea of law as consensual belief (hallucination), Ludlow moves into assimilating the adoption of laws by the citizens (what Hart ([9]) called the “internal point of view”) to the attitude that members of the Internet communities have towards the regulations of such communities. This assimilation allows for the possibility of switching loyalties from one to the other set of norms.

The idea was that it is easy to dismiss a VR [virtual reality] world as a joke if it is run by wizards, but what happens when VR worlds develop systems of justice that are more fair than those we encounter in the RW [real world]? Or what happens when we encounter VR worlds in which there is no discrimination? Or VR worlds in which no policy is established without the unanimous approval of the denizens of that world? Which world begins to look clownish at that point? And where will we prefer to spend our time and conduct our business?

Would such a switch be possible? To evaluate it, we need to consider that Ludlow is right in so far as he connects law with beliefs: law is “a kind of consensual hallucination”, he writes. This connection holds not only between cyberlaw and beliefs: it holds between beliefs and law in general and in any field of law (private law, public law, criminal law, etc.). The connection properly holds between beliefs and norms, any kind of norms (legal norms, moral norms, norms of etiquette, etc.). This implies that the connection between beliefs and law holds as far as law is made up of norms.

However, as we shall see, law is made up not only of norms (which are an essential part of law), but also of force, namely military power controlled by courts and other agencies (which is also an essential part of law). From this perspective, it is questionable whether cyberlaw may be properly considered law if it is made up only by beliefs (namely only by norms) and not also by force. It may be doubted that pure beliefs, without the support of force may be sufficient for imposing a social order, as it is necessary in particular for the protection of civil rights.

Let us now try to clarify what we mean by a belief. We may say that a belief is the engagement that, for any reason and to all possible effects, we have towards an idea. Since ideas are distinguished, inter alia, between theoretical ideas and practical ideas, the same distinction holds between theoretical beliefs and practical beliefs. In particular, a norm is a practical belief, in particular the belief that a certain pattern of behaviour ought to be performed under certain circumstances (Pattato [19]).

Here is how the idea of a belief was expressed in the history of philosophy.

For Aristotle ([2], On the soul, 428a 20): “Opinion (doxa) implies belief (pistis), for one cannot hold opinions in which one does not ”

For Aquinas ([1], Summa Theologiae, II, 2, q. 2, a. 1), on the track of Augustin: *Credere est cum assensione cogitare.*

For David Hume ([11], V, 2):

Belief is something felt by the mind, which distinguishes the ideas of the judgement from the fictions of the imagination. It gives them more weight and influence; makes them appear of greater importance; forces them in the mind; and renders them the governing principle of our actions.

The difference between fiction and belief lies in some sentiment or feeling, which is annexed to the latter, not to the former, and which depends not on the will, nor can be commanded at pleasure. It must be excited by nature, like all other sentiments; and must arise from the particular situation, in which the mind is placed at any particular juncture

Finally, Franz Brentano ([5], II, 1) said that: “An object of judgement is present in two ways in our mind: as a represented object and as an accepted or denied object”. When an object is accepted or denied, it is believed.

Normative beliefs, beliefs and something has to be done, when appropriate circumstances obtain, are an essential component of social organisation. However, the law is a mix of norms and force: it is a cluster of beliefs eventually enforced by organised power. Enforcement is (unfortunately) necessary since we may have different normative beliefs, and anyway we may give priority to our individual interests over our normative beliefs: unless one body or rules (hopefully good ones) are enforced, chaos is inevitable. Therefore, the need of enforcement puts the idea of the law of cyberspace into a dilemma.

If cyberlaw is going to be enforced through organised power, than it will become law, with the authoritarian aspects which characterise any type of law. The idea that “no policy is established without the unanimous approval of the denizens”, needs to be substituted with the complexities of political processes.

If cyberlaw is not going to be enforced then it will be disregarded by individuals and - notice - by States and other agencies who are endowed with organised power: namely, mafia, terrorism, and dealers of children, women and men.

In conclusion we must not be illuded that the novelties introduced by the Information Society may avoid the thousand and thousand-year-old problem of the relationship, better of the contrast, between law and freedom: also in cyberspace law (norms supported by organised force) on the one hand, may be may encroach upon freedom, on the other hand, is freedom’s necessary precondition.

The illusion that cyberlaw may not need the support of organised force illusion has a name: utopia, which means nowhere, in no place at all, neither in cyberspace you may have freedom without law, namely without organised power.

In the following we are going to substantiate this conclusion by analysis what role the law had in the history of the Internet, and what role it may have in its future.

3 Regulating the Internet

To establish the role of the law in the Internet, we will move from Lawrence Lessig (Lessig1999co, Lessig1999lh), well-known distinction of four ways in which cyberspace can be regulated:

1. The law, that is, as we saw, those norms which are imposed through organised coercion. As Lessig ([14], 508), says copyright, defamation, obscenity law all continue to threaten ex post sanctions for violations in regard to behaviour taking place in cyberspace.
2. “Norms”, by which Lessig means those rules which are adopted by the members of a community, and which are imposed through non-organised sanctions.
3. The market, that regulates (influences) behaviour by assigning prices to the facilities and opportunities available in cyberspace (access to sites and contents, advertising, etc.)
4. The “code”, and by which Lessig means the hardware and software supporting (constituting) cyberspace.

Here is how Lessig ([14], 508 f.) describes what he calls the code, and how it performs its regulatory function:

The code, or the software and hardware that make cyber-space the way it is, constitutes a set of constraints on how one can be-have. The substance of these constraints varies - cyberspace is not one place. But what distinguishes the architectural constraints from other constraints is how they are experienced. As with the constraints of architecture in real space - railroad tracks that divide neighborhoods, bridges that block the access of buses, constitutional courts located miles from the seat of the government - they are experienced as conditions on one’s access to areas of cyberspace. The conditions, however, are different. In some places, one must enter a password before one gains access; in other places, one can enter whether identified or not. In some places, the transactions that one engages in produce traces, or “mouse droppings”, that link the transactions back to the individual; in other places, this link is achieved only if the individual consents. In some places, one can elect to speak a language that only the recipient can understand (through encryption); in other places, encryption is not an option. Code sets these features; they are features selected by code writers; they constrain some behavior (for example, electronic eavesdropping) by making other behavior possible (encryption). They embed certain values, or they make the realisation of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates.

Lessig's idea that the four factors indicated above, and particularly code, shape behaviour in cyberspace provides a powerful model for the legal analysis of the Internet, and we will extensively refer to it in the following pages. On the terminological side, however, we prefer to use the word norms for referring to both legal and non legal norms: both of them share the fact of being practical beliefs. To mark their difference we prefer to speak of legal norms and social norms (where "social" means simply "non legally enforceable").

Also using the expression "code" to refer to the hardware and the software of the net can be questionable. What the user of the net has to deal with are computational processes, processes which are performed by hardware governed by software. Such processes do not proceed randomly: they follow certain stable patterns, in a way that is similar to the ways in which nature's working follows causal patterns. These patterns, however, are usually the result of human design. At the lowest level computational patterns followed by computer systems correspond to single programming instructions (they are data processing operations which are prescribed by such instructions). At a higher level, they correspond to input-output functions performed by combinations of programming instructions and data (consider how an e-mail is sent, or how a web page is visualised, how an encrypted message is produced). At a higher up level, they correspond to properties of certain procedures (consider how a procedure sending a message may structure it according to certain communication protocols). Finally, they correspond to the ways in which the various objects populating cyberspace (characters in a videogames, web services offered on the net, software agents) appear and behave, i.e. to the properties and methods which characterise those objects. To express all patterns of functioning of (computational processes over) computer systems, we may generally speak of "virtual rules" (in a similar sense, Reidenberg ([21]) speaks of *lex informatica*). Therefore, use denote as virtual rules all of those: operations performed by single programming instructions, computational functions performed by complex programming procedures, the abstract criteria (standards and protocol) that such procedure respect, the properties and the methods characterising complex objects. Virtual rules are different from legal and social norms (which directly regulate human behaviour) in that they express patters of behaviour and properties of computational processes, and they usually correspond to design specifications of those processes. Computational processes (and therefore virtual rules characterising them) are relevant to our behaviour in cyberspace since:

- they enable us to certain types of actions and interactions (we can act in cyberspace only by activating appropriate computational processes);
- they determine how easily (with what burdens) those actions can be exercised
- they determine what information will be provided to humans concerning the available actions

- they may link (unintended and possibly unknown) side-effects to the actions they enable;
- they provide the context in which these actions are performed.

So, as in the physical world there is an inevitable primacy of physical laws over human laws (in the sense that the physical laws, by determining what is physically possible circumscribe the domain of what may be legally requested)⁷, similarly in cyberspace there is a primacy of virtual rules, since those rules determine what is “virtually” possible (what is possible in the virtual worlds which are constituted by computational processes over the net). Once virtual rules fix what actions are virtually possible, under what conditions, and in what ways, then the market may put prices for obtaining other people’s cooperation or consent in performing those actions. Finally, social rules, may qualify as admissible or non-admissible (in certain context and communities) some of the actions which are enabled by virtual rules and priced by the market. Similarly the legal rules may qualify virtually possible actions as being legally permissible or mandatory, or forbidden.

Therefore, in a first sense, virtual rules, the “natural” laws of virtual environment(s), condition every form of regulation, providing the matter to be regulated (virtually possible actions).

Moreover, virtual rules condition the possibility of enforcing social or legal norms. For example, if no way is available for having secure transactions and for stopping access and duplication of intellectual property, there is little chance of using the Internet as a marketplace for cultural products. Similarly, if anonymity is enabled (if no way is available of identifying who started certain computational processes over the net, and particularly transmitted certain information), then the operations of the law (which is based upon publicly organised coercion) become difficult or impossible.

On the other hand the primacy of virtual rules is questioned by the fact that computational processes are a human creation (in most cases) or at least they can be modified through human intervention. This means that the market, and social and legal norms as well, can react on virtual rules, by inducing their modification. Consider how the market is continuously reshaping the hardware and software infrastructure of the net, according to its needs: new commercial sites are open, new software application for e-commerce are made available, new techniques are developed for securing on-line transactions, for protecting intellectual property, for monitoring customer’s behaviour, for extracting information from the net.

Also social rules and values contribute to the evolution of the computational infrastructure: consider how, in certain Internet communities, inspired to the so called hacker culture, the open source movement has led to the development of substantial software projects (the GNU-Linux project, first of all), or how software may be developed for protecting anonymity and privacy.

⁷This is expressed by the legal saying “ad impossibilia nemo tenetur”.

Finally, the law itself can impose certain virtual rules, for example, by forbidding the use of certain algorithms (as for the French attempt to ban cryptography), by imposing specific algorithms (as in the US attempt of embedding the so called Clipper chip for cryptography in every PC), by requiring that computational processes are performed in such a way as to ensure security and privacy or that certain data are stored and other data are deleted (as is the case according to European data protection laws), etc. All those regulations introduce obligations that cannot be directly implemented through human action alone: to comply with them requires modifying the computational behaviour of computer systems, i.e. implement virtual rules that match those legal requirements.

The idea that there are various factors at work in shaping the Internet allows us to understand better what is at stake when we are discussing whether the law should govern the Internet: the choice is not that between law and individual freedom. The choice is between an Internet that may be shaped also by the law (along with other factors,), and an Internet which is only shaped through other factors (social norms, markets and virtual rules). This is what we will consider in the following paragraphs.

4 The beginnings of the net

On the basis of the model we described in the previous section, we will try now to consider the evolution of the Internet and the role that norms have played in it, in their interaction with virtual rules (with the technical infrastructure).

The Internet was born, as everybody knows, from a combination of multiple factors: a financial contribution from agencies linked to US defence, the involvement of young and creative scientists, open discussion and experimentation in academic environments. In this context the basic architecture of the Internet was defined through a choice in favour of neutrality and freedom in communication. The basic net protocols (TCP/IP), i.e. the basic virtual rules of the Internet, define a computational infrastructure where any message can travel from any node to any other node, without intermediate controls. In fact every content, be it a technical report, a music, a picture, a movie or a program, is divided into packages, each of which is included in a digital envelope, indicating all information that is necessary for transmitting the package to its destination. Packages follows different and non pre-established pathways, being sent forward, closed in their digital envelopes, by computers called gateways or routers. Only at the destination computer, envelopes are opened, packages are reassembled and checked (to verify whether there have been transmission errors, and possibly ask for retransmission). This architecture grounds the possibility of free, uncontrolled, equalitarian communication.⁸

⁸Here is how Naughton[17], 163, presents this aspect of the Internet: “the Cerf-Kahn idea of a gateway linking different types of networks was the key both to the subsequent growth of the Internet and to the explosion in creativity which it fostered. Its emphasis on ‘end to end’ reliability meant that the network would essentially be indifferent to what is was used for. The gateway had only one task - that of getting packets from one place to another. They

The lack of intermediate controls has also meant that the net, from its very beginning has tended to become a global means of communication, where physical locations, and geographical borders were irrelevant. The openness and neutrality of the original Internet architecture have been key factors in fostering its creative developments. The net became the flexible environment where its users (who were mostly computer experts) could project new, unexpected applications and contribute to their development. In this context, the main services provided by the net (e-mail, bulletin boards, file transfer, and the world wide web) could emerge. Here is how Naughton ([17], 138) describes the ethos that accompanied the origins of the net:

What those kids were inventing, of course, was not just a new way of working collaboratively, but a new way of creating software. The fundamental ethos of the Net . . . was an ethos which assumed that nothing was secrete, that problems existed to be solved cooperatively, that solutions emerged iteratively, and that everything which was produced should be in the public domain. This was, in fact the genesis of what would become known much later as the Open Source movement

More generally, the Internet has been shaped by different cultures. As Castells ([7], 37) observes:

the culture of the net is characterised by a four-layer structure: the techno-meritocratic culture, the hacker culture, the virtual-communitarian culture, and the entrepreneurial culture. . . . These cultural layers are hierarchically disposed: the techno-meritocratic culture becomes specified as a hacker culture by building rules and customs in to networks of cooperation aimed at technological progress. The virtual communitarian culture adds a social dimension of technological sharing, by making the Internet a medium of selective social interaction and symbolic belonging. The entrepreneurial culture works on top of the hacker culture, and on the communitarian culture, to diffuse Internet practices in all domain of society by way of money making”

At the beginnings of the net, when it was used by a limited number of people, often involved in its construction, what Castells calls the techno-meritocratic and hacker cultures were certainly its dominant shapers. The Internet appeared to its users to be an environment which offered new unexplored possibilities of action, interaction and cooperation, possibilities that it was up to them to identify and develop, in a cooperative effort. In such a framework, authority would belong to people that on the one hand possessed superior technical and scientific competence (as recognised by their peers), and on the other hand were available to use this competence for advancing common cooperative projects.

cared nothing for what those packets represented. As far as the network was concerned, a packet containing a fragment of a love letter was the same as one containing a corner of a pornographic photograph of a segment of a digitised telephone conversation.”

The logic of the law, and in particular, recourse to politics for stating binding rules of behaviour, and to physical coercion for implementing them, was out of place: shared rules ought rather to be defined by competent and co-operative technical choices, and to be consensually implemented.

The net culture succeeded in an admirable way to reconcile creativity and co-operation, so that innumerable inventions were implemented into a rich and varied shared communication infrastructure. In such a context co-ordination was obtained through non legal instruments.

Firstly, there was the technical and moral authority of the founding fathers of the Internet (as, among others, Vinton Cerf, Robert Kahn, e Jon Postel).

Secondly, there was the mechanism of the creation of standards and in particular of communication protocols (the rules according to which messages must be constructed and interpreted). The “normativity” of standards generally results from everybody’s need to behave in a way which is coherent with others’ behaviour, to participate in communication.⁹

Therefore, what pushes an individual to adopt a standard is not the specific merit of that standard (the comparative advantage it would provide, if adopted by everybody, in regard to other possible standards). The individual choice of following a certain standard is only justified by the standard’s chance of being generally followed. Therefore, the real power is in the hand of those who, through their choice of promoting a standard are able of making it “salient” to everybody, i.e. such that everybody expects that everybody else will follow it (on salience, cf. the classical contribution by Schelling ([23])). Ability to provide salience provides a power that does not require legal or a moral sanctions: self-interest is enough to bring people to converge on salient standards. However, this mechanism allows for a possible contradiction between collective and individual rationality: the first would require all users to jointly adopt the best standard (the one which would be most beneficial to each one, if adopted by everybody), and individual rationality, that demands each one to follow whatever standard one expects others will follow, regardless of its comparative merit. At the beginnings of the Internet, the match between collective and individual rationality was ensured by the ways the Internet community had of producing saliency. Saliency of a protocol would be determined by its adoption by committees of impartial experts (after debates in the Internet community), on the basis of the technological appropriates of the chosen protocol, having regard to the shared goal of communicating and sharing resources over the net. Decision by the appropriate committee (such as the IETF-Internet Engineering Task Force) made the adopted protocol salient to the Internet community, so that each software developer would adopt it, in the expectation that all other developers would do the same.

Besides the conventional “normativity” of protocols (note that protocols are

⁹Using the jargon of game theory, we may say that standards provide solutions to co-ordination games, situations where everybody prefers to adopt the same pattern of behaviour that others will adopt, rather than going on his or her own way, but there are different possible candidates for shared adoption. Protocols are conventions in the sense described by David Lewis([15]).

not proper norms, since their efficacy may only rely on self-interest), the Internet community produced also norms *stricto sensu*, i.e. shared beliefs that certain patterns of behaviour ought to be followed by each individual (in the interest of a community or to achieve the common aims of its members), even when this would be against the interest of that particular individual. Such shared normative beliefs are usually combined with informal sanctions consisting in the negative judgement of the community, a judgement which may lead in serious cases to stigmatising or even ostracising violators. This type of normativity is expressed by netiquette rules (e.g. rules such as those prescribing not to send advertising to news groups, or not to engage in offensive exchanges, or flaming), and, in a more serious way, in those rules which discipline cooperation in non-commercial projects, as one can find in some versions of the so called hacker's ethic (obligation to contributing to the projects one is participating in rather than just taking from them, prohibition to use its result commercially to the detriment of the project, etc.).¹⁰

In such cases, one is requested to avoid exploiting one's fellows, i.e., to give priority to shared rules over self-interest (not exploiting the compliance of one's fellows). In sufficiently tight communities such norms do not require legal sanctions: the stigma carried by the negative judgment of the community, plus the possibility of being excluded from future co-operation may suffice to ensure a sufficient level of compliance.

This combination of shared conventional protocols and social norms was sufficient to govern the Internet at its beginnings. The law had a marginal role: it provided the property rights over the hardware of the net (the software being generally freely available), and it provided background rights (freedom of speech, communication, private initiative) which enabled people to make decentralised and creative use of the possibilities offered by the computational infrastructure of the net.

A further limitation to the legal governance of the Internet consisted in the fact, that as we observed the architecture of the net enabled for uncontrolled global communication. This reduces the possibility that national laws can block access to what is available on the net: every object which is made available on the net can be accessed in principle by everybody, regardless of the physical location of the hardware where it is located. This determined the failure of the first attempts to block the circulation of information which was illegal accord-

¹⁰To refer again to elementary game theory such norms are intended to provide solutions to prisoners-dilemma structured situations, i.e. to situations where (a) every member of the community would prefer that everybody follows certain shared rules, rather than everybody acts independently, but (b) one may take advantage from individual deviant behaviour (at the other's expense), when all others are complying. More exactly such situations are characterised by the following patten of egoistic preferences: each one's egoistic first choice is the situation where one is the only violator, to the detriment of one's complying fellows; one's second choice is the situation where all (including oneself) are complying; third choice is the the situation where nobody is complying (for a more detailed and precise discussion, cf. Ullman-Margalit([24])). Consider the situation where all other members of a group are contributing their efforts to a shared open source project, and one packages the results into a commercial product one sells individually. Consider also the situation where one exploits a discussion group established under non commercial premises for advertising).

ing (only) to the law of certain countries. Illegal (pornographic, racist, nazi, criminal, etc.) information could simply be transferred to other sites, located on computers placed in States where such information was legal. This process was facilitated by the fact that most of the Internet infrastructure is located in the US, where freedom of speech enjoys strong constitutional protection.¹¹

5 The net loses its innocence

The model we described, where Internet is (and ought to be) a domain of unfettered freedom of communication, ensured at the technical level by the virtual rules (the protocols) implemented in its architecture, and at normative level by the mores of its community, gets into trouble in the '90s, when the net is accessed by larger sections of the world population, and is colonised by economical interests.

The explosive growth of the net and the increasing diversity of its users put into question the very idea of the existence of an Internet community, as a group of people involved in a shared project and accepting shared norms. When diversity is so great that the net contains both students of renaissance art and rape lovers, fighters of racism and hate preachers, defenders of “family values” and supporters of paedophilia, we must conclude that there is no overlapping consensus among the users of the net able to support an all-inclusive Internet community (on the idea of an overlapping consensus, cf. Rawls ([20], 133 ss). At most all Internet users may share an interest in free self-organisation of the net, as a precondition to pursuing one’s particular values within one’s particular community. Rather than as a community, the Internet appears to be, at best, the “framework for Utopia” described by Nozick ([18], 297 ff.), that is an empty space where everyone can try to build, with whatever joiners one may find, a circumscribed community corresponding to one’s preferred values and interests. Such possibility of practicing freedom of association on a planetary scale is an important value. However, we should not overestimate the normative function of such communities: their diversity, their partiality, their multiplicity, their precariousness questions their ability to provide checks to antisocial behaviour in the Internet (spamming, spreading viruses, damaging computer systems, etc.) and to using the Internet for preparing antisocial behaviour to be implemented in the real world (terrorism, paedophilia, sexual tourism, etc.).

The second, and the main factor determining the loss of the innocence of the

¹¹As Castells ([7], 169) observes: “Because the backbone of the global Internet was largely based in the United States, any restriction to servers in other countries could generally be bypassed by re-routing through a US server. To be sure, authorities in a given country could detect the recipients of certain types of message by exercising their surveillance capabilities, and then punish the offenders according to their law, as Chinese dissidents have often experienced. Yet, the surveillance/punishment process was too cumbersome to be cost-effective on a large scale, and in any case, it did not stop Internet communication, simply imposed penalties upon it. The only way to control the Internet was not to be in the network, and this rapidly became too high a price to pay for countries around the world, both in terms of business opportunities and access to global information”

net was its increasing use for economical activities. This introduced into the net new powerful actors, values and practices, and determined a fundamental change in its social function. The original architecture had a dual attitude towards the market. On the one hand, its neutrality (its ability to convey whatever content to whatever destination) allowed it to become the ideal place for the creative development of new economical initiatives, concerning all aspects of the economy (advertising, exchange, communication, organisation). Other aspects of this architecture, however, hindered its use for commercial purposes. In particular, the openness of the net made it difficult to ensure identification of the parties in commercial transactions and security of their communications. Moreover, free access to every object available on the net clashed against its use for the commercial distribution of cultural products (on this function of the net, cf. Rifkin ([22])).

The colonisation of the net by business determines the failure of the mechanisms for the autonomous regulation which were previously at work. So, the definition of standards and protocols, rather than emerging from open and competent discussions, according to the impartial judgement of a scientific committee (such as IETF), tends to result from battles and compromises between competing commercial strategies. The mechanism of convention (the need to do whatever each one expects others will do) still pushes individual users or programmers to adopt dominant standards. However what standards will dominate the market depends on the market share (and power) of their supporters. Even when it is clear that different protocols (rather than those supported by the market leaders) would bring higher benefits (if they would become shared standards), individual users are powerless: their own individual interest pushes them toward expected winners. No individual escape from imposed conventions is available: only a social choice, a joint commitment (on the basis of a shared preference) could give salience to a different option, and contrast the dominance of market forces.

Let us now consider the formation of proper norms, that is beliefs that certain behavioural patterns should be followed, even when the concerned individual could profit from his or her deviance. What made the original Internet a fertile ground for norm formation, besides the existence of an Internet community, was the fact that members of this community tended to share the same roles: everybody would be both a sender and a receiver of information, a provider and a reader of contents, a software developer and a user of software developed by others. This provided a commonality of interest that could support the formation of a “common point of view”, i.e. the shared perception that certain patterns of actions (when generally followed) would benefit all (though individuals still, as it usually happens in prisoner-dilemma structured situations, needed to be checked from occasionally exploiting other people’s compliance). This perception would lead individuals to share corresponding norms.

However, when organised business takes over, an economic landscape emerges where different groups (and organisations) play distinct and non-interchangeable roles (producers vs consumers, providers of contents vs readers, software developers vs users). Each of those groups tends to be characterised by specific

group-interests, sometimes converging and sometimes competing with the interest of other groups. Under such circumstances, group interests and points of view still favour the emergence of normativity, i.e. the shared adoption of rules requiring each member of the group to follow patterns of behaviour the general compliance of which would benefit all members of the group. However, such norms do not necessarily benefit outsiders to that group, so that genuine conflicts between competing group interests may arise. Consider for example, electronic commerce. When the regulation of the behaviour between merchants it at issue (e.g. ways of conducting with efficiency and security business to business electronic transactions), spontaneous *lex mercatoria*, possibly specified and even enforced by the institutions of the merchants' community, will usually provide appropriate solutions, benefitting not only merchants but also society as a whole (though conflicts of interests between different groups of economic operators should not be underestimated). However, in other domains, such as for example in privacy protection, there is genuine conflict of interests between on-line merchants and customers (the first benefitting from the largest possibility of monitoring on line behaviour and using personal data, while the latter benefitting from being ensured privacy and control over their data). Consequently is very unlikely that *lex mercatoria* (or, more generally, any one-sided self regulation) may provide a discipline which is acceptable for customers as well.¹²

Similarly, there is a clear conflict of interest between commercial providers of software e cultural products and those pre-existing communities on the Internet (such as the hackers' and the open-source movements) who have been practicing on the Internet alternative ways of producing, accessing and using what is now being offered within the usual commercial paradigm. It is very hard to see how self-regulation could provide a solution for such conflicts of interests, or whether these are wars where, to use the famous words by Hobbes ([10] I, 130 "Force and fraud are . . . the two cardinal virtues" (consider for example the recent attempts, by leading commercial producers, to make software patentable in order to stop open source).

6 The new architecture of the Internet

Since the network has expanded and commercial interests have entered it, the failure of self-regulation has led to various requests for legal interventions. Some of these requests have been successful, leading to new statutes or to adaptations

¹²One may argue that it is in the interest of merchants to provide a minimum of on-line privacy protection, since total lack of privacy would keep customers away from the Internet. However, one cannot expect self-regulation on the merchants' side to offer any level of privacy protection which goes beyond that minimum (that can be very low indeed). Moreover, from the merchants' perspective, it would be even better if there was just an appearance of privacy protection, rather than real protection, so that consumers would continue to shop, and merchants would continue to collect and process their data. The connection between group interests (or "class" interests, as once people used to say) and *lex mercatoria* is extensively considered by Galgano ([8]).

of case law. Consider how the law has changed to ensure legal validity of on-line contracts, to provide a legal framework for electronic signatures to provide a strong protection to copyright, to allow algorithms and business methods implemented in software to be patented, to sanction the unauthorised use of trademarks and commercial names. This legal intervention, though achieving significant results (as in overriding Internet rules for assigning domain names), was in same regards hindered by the nature of the net: on the one hand by its global extension (as opposed to the geographical boundaries of national legal systems), and on the other end, by its uncontrollable architecture (as opposed to the need to detect violations and identify and punish their authors).

In recent times, the attempt to overcome such limitations (and some intrinsic limitations of the law, such as its rigidity, and the costs of its application) have led to new technological developments. Market forces, after using the environment provided by cyberspace (its virtual rules) to do business, have started to modifying it so that it better fits their needs. This is done through modifying the architecture of the Internet, in ways that, unless adequate public constraints and controls are introduced, may endanger the role of Internet as a medium for free communication (this thesis is extensively developed by Lawrence Lessig ([13], [14])).

This process consists in further enriching the architecture of the net, by layering, on top of the original Internet protocols, new protocols and software applications, which embody new virtual rules. Those virtual rules operate at two levels.

At the first level, actions that are not wanted by the “owners” of an area of cyberspace, or by the providers certain contents, are disabled by appropriate virtual rules. Rather than requesting the law to forbid certain actions under certain conditions, appropriate computations, outside the control of the user, can make those actions impossible. This process is particularly evident in the domain of intellectual property, where software controls are displacing the law: this may happen both by restricting what one is able to do while interacting with a site e.g. making downloading impossible, or providing selective access, or by embedding into purchased goods checks which allow only for the precise type of usage which corresponds to the seller’s intention (e.g., using a music track for a certain time span, a certain number of times, on a certain computer, etc.) For a consideration of how this is displacing traditional copyright law and, in particular, the doctrines of fair use, cf. Lessig [13], 122 ff.). More generally, this approach leads to substituting the category of the legally permissible with the category of the virtually possible: one is allowed to do whatever one, as a matter of fact, can do, when interacting with a site or using a certain product, but one can do only do what one had been enabled to do. Behavioural restrictions enforced by software can become more and more selective, as computing applications acquire more and more intelligence. In a future that is approaching intelligent software agents, embedded into software applications, may flexibly decide, according to the circumstances and previous behaviour of the user, what user’s actions to enable and what actions to disable. In a context where virtual rules are substituting legal constraint and technological possibility is substitut-

ing to legal permissibility, the law is appealed to, not as a restraint on the behaviour of the users, but as a restraint of the behaviour of hackers, trying to crack control techniques. So, rather than to punish unwanted behaviour, the law is requested to punish (with extreme severity) those who enable such behaviour.

At the second level, various technologies of personal control are embedded into the Internet, technologies for identification of people, for their surveillance (for recording their actions), for investigation (for processing data which have been collected). Here we cannot consider what these technologies are, which include a vast array of tools, going from cookies, to biometric identification procedures, to data mining algorithms. Let us just remark that all these technologies may be used in ways which are highly useful to society, but also in ways which are extremely dangerous. Consider, for example double key cryptography, one of the major technological achievements of the last decades. As it is well known, this technology offers two possibilities: on the one hand, the possibility of hiding the content of a message in such a way that only the addressee of the message can read it (this is done by encoding the message with the public key of its addressee), on the other hand, the possibility of identifying with absolute precision the sender of a message (this is done by coding an abstract of the message with the private key of the sender). Therefore, double key cryptography is able to contribute both the use of the Internet both for interpersonal communication and for doing business: on the one hand it provides secure secrecy in communication (as needed in personal communication and also in business contacts), and on the other hand it ensures identification of the parties (as required in commercial exchanges). It is approaching the time where one will be requested, whenever entering any area of the Internet, to provide one's digital signature. This will provide for secure identification which, combined with electronic monitoring, will allow any person to be attributed every detail of his or her on line behaviour.

In regard to how virtual rules embedded into commercial software limit the freedom of the user, one also needs to consider that those rules often work secretly, they describe properties of computational processes that are often not observable by their users. In fact, instructions of most commercial software packages are unaccessible to the user (their source code is not provided, and in most legal systems it is even forbidden to try to decompile the executable code). Nor higher level descriptions of such packages provide the user with all relevant information (one can never be sure that this is the case). Therefore, one cannot know what the software one is using is really doing, which means that one cannot fully anticipate all effects of one's actions, and the context in which one is performing them. One interesting example concerned a feature of widespread program for accessing on-line music and movies, which informed the producer of any piece the user would download (without telling the user that this was being done).

Finally, consider that no technological constraints prevents that techniques of identification and control now being used in commercial spaces, are taken over by national governments, possibly joining forces to obtain reciprocal co-

operation (so, “big brother” and “big browser” could join forces). Even in this regard, one needs to take a nuanced approach. Police controls over the Internet may be fully justified by the need to prevent serious crimes (terrorist attacks, pedophilia, ecc.), though the dangers of the Internet in this regard have probably been overemphasised. However, assume that all individuals were provided with digital signatures, and that all access providers were requested to allow access to the Internet only to people who were identified through their digital signature, to trace all their on-line behaviour, to store all those data, to give access to it to the police. A further element of such a global control would consist in the possibility that public authorities of different countries freely exchange such data, as is foreseen to a large extent by the Cybercrime convention, (Budapest 23/11/01). Under such circumstances the Internet could become a place of total control. Possibly, cyberspace would no longer (or to a lesser extent) be the domain where, protected by the Gyges’s ring of anonymity, individuals may engage in illegal and malicious behaviour. However, the Internet would become a global panopticon, when every action will be observed, recorded, and evaluated. It obvious how this would have serious impact on the exercise of basic human rights, such as the right to express and communicate one’s opinions.

7 Conclusion

It is now time to try to draw some conclusions from what we have been saying so far. Following Lessig ([13]) approach, we have considered how legal norms may be only one of the factors that concur in shaping cyberspace. We have also seen that in a global context characterised by expanding diversity and powerful commercial interests the spontaneous or anarchic evolution of the Internet tends endanger values of freedom, openness, cooperation, research, which characterised its beginning. If the law remains silent, other instruments of control are going to take over the cyberspace. These instruments (their virtual rules) on the one hand are global, since they apply to every user of the system embodying them, i.e. to the particular area of the cyberspace which is created and managed by that system. On the other hand they are local, since they concern exactly that particular system and area, and they express the specific needs and policies of its owner. They may provide arbitrary degrees of sophistication in governing human action and they can make use of all knowledge that can be extracted and processes by computer systems.

One may ask whether we should not accept with enthusiasm this trend, and accept the fact that the law is being displaced by more sophisticated forms of social control. Through computer-based governance the old utopian dream of overcoming the law may become reality. Rather than using normativity to restrict the behaviour of an agent (which requires the active co-operation of the mind of the agent, and calls for his or her endorsement of the norm, or alternatively for his or her fear of the sanction), society could govern human behaviour by refined computational processes enabling only permissible actions. As we observed above, in regard to new ways of protecting intellectual property,

there would be still the need to legally prohibit only behaviour which attempts at stopping those very computational processes (e.g. hacker's attempt to crack software protections). Clearly we cannot exclude in general the possibility of restricting one's behaviour when interacting with a computer system. Such limitations may be opportune and even necessities, also for protecting legal values. Consider for example, how protection of privacy of health data

However, there are strong reasons for believing that the law should still be in control of cyberspace, at least to some degree.

The first reason concern the cognitive nature of the law. Legal norms, to work properly, need to become people's beliefs, and therefore need to be interpreted and understood. This requires some cognitive efforts from the concerned people, but also empowers them: they know what the law requires from them, and they may find or negotiate strategies for coping with such requests. This is not necessarily the case for virtual rules, which are to be applied by computer machinery without the concerned persons even knowing of their existence.

The second reason, especially in democratic legal systems, concerns the connection between law and politics. Legal rules result from political processes, as solutions adopted in order to achieve public objectives. This means that those to which certain rules appear to be wrong (not to contribute to the "common good", whatever is intended by this locution) may question them, and possibly start political processes that may lead to legal changes. This is not the case for virtual rules, which are usually decided upon in the private domains.

The third reason concerns the normative nature of the law. Legal beliefs (being beliefs to the effect that something ought to be done and ought to be enforced) have a strong connection with beliefs concerning justice, i.e. the appropriate way of regulating society and of balancing competing interests (and in particular with conceptions of justice that are reflected in constitutional values). This has a bearing on the interpretation of the law, which needs to take into account also such considerations. This is not the case for virtual rules, which are to be implemented by computational processes, according to unilateral specifications.

The fourth reason consists in the connection between the law and the idea of equality or impartiality. This means that reference to the interests of one party is not a sufficient justification for a legal decision, when other people's interests are unduly sacrificed (though different views of what interests deserve protection and of their priorities are possible). This is not the case for virtual rules, which are defined only on the basis of the interests of those who have developed a computer application, and which are applied by computer systems.

The fifth reason is the connection between the law and public dialogue, democratic deliberation. Legal norms, as ways of coordinating human behaviour for achieving public aims, can be the object of public discussions, where reasons for and against their adoption (or their conservation) needs to be considered. This is not the case for virtual rules, which are adopted in consideration of private interests, regardless of other people's opinion about them.

The sixth reason consists in the fact that, as we said above, the law consists of norms that are to be implemented (when necessary) through organised force.

This may be viewed a negative aspect, since physical force, or violence as one may call it, is the most direct and brutal form of influence humans may exercise upon other humans. However, in civilised societies, the legitimate use of violence has been monopolised by the State, and generally can be legitimately applied only through public judicial procedures. This means when one party decides to appeal to the law, it must be ready to submit itself to the judicial procedure, a procedure where the other party may also express its reasons and a public impartial judgement is expected to be given. Compare the judicial process, with all its defects, to what private enforcement may be like. Consider for example what type of “enforcement” would be authorised by the recently proposed US Peer to Peer Piracy Prevention Act, which would allow owners of intellectual property take the law in their own hands, and attack (by using various hacking techniques) those sites that distribute copyrighted materials without authorisation.

What we have said so far does not imply that the law should attempt to directly regulate every aspect of the Internet, according to some particular view of the public interest. Public interest is best served by allowing the Internet to be a place for free global communication, and free economical initiative: both the creativity of a global dialogue and the creativity of a global marketplace must coexist and possibly stimulate each other, as they have done so far to a considerable extent.

What we may say in this regard is that law’s role should be that of preserving the pluralism of the net, to make so that in it all of the following can coexist: free communication and commercial activity, humanitarian activities and search for profit, democratic debate and pure entertainment. It is possible, however, that the law goes in the opposite way, promoting the development of a one-dimensional net, consisting in a combination of controlled private spaces where consumption and profit would be the dominant and possibly exclusive aspects. This is the trend which is favoured, for example, by rules providing for a stricter protection of intellectual property and, in particular, for the patentability of software inventions.

We cannot here consider in detail how the law should try to govern the Internet (for some very interesting general ideas, cf. Lessig ([13], 122 ff)). Let us just remark that this depends on the nature of the relationships to be regulated. In certain areas, as in the data protection, a detailed legal regulation (following the model of the European privacy laws) is required to ensure a minimum of on-line freedom. Similarly, explicit statutory regulations are required for consumer protection, and for ensuring fair use of cultural products. In other domains, such as in business to business relationship, the law should rather stimulate self-regulation, possibly lending its support to norms emerging from the merchants’ community. In the establishment of standards and protocols, rather than imposing solutions, the law should try ensure that all different interests are represented in decisional processes, so that fair (and competent) choices can be made. Endorsement of practices which promote certain legal values may also require ways of public involvement which are different from legal regulation, such as adopting (also) open source software in public administrations and

promoting its knowledge.

So, to conclude our presentation, we will reaffirm what we said in the beginning: there is a need for the public interests and values to contribute to shaping cyberspace. Politics and law are the traditional ways in which those interests and values can be articulated and legitimately imposed. We need a political and legal action at the global level to preserve and develop in cyberspace the values which our laws have been promoting so far in the physical space. We should not be too pessimistic concerning the possibility of realising legal initiatives at a global level. The “code” and its virtual rules are already working at a global level, quite effectively. Moreover, we can see that whenever strong commercial interests have been at issue (as in the protection of software and intellectual property, in the prevention and repression of cybercrime, in promoting electronic commerce) appropriate legal actions have been taken at the appropriate level with little delay: international conventions have been signed and co-operation for enforcement has been put in place, statutes have been enacted, decision have been taken. There are no unsurpassable reasons why also in other areas, such as privacy protection, freedom of information, and consumer protection (intended in a large sense) this cannot be the case.

References

- [1] Aquinas, *Summa theologica*, Thomas More Publishing, Allen (Texas), 1987.
- [2] Aristotle, *De anima / on the soul*, Penguin, Harmondsworth, 1987.
- [3] Robert Axelrod and Michael D. Cohen, *Harnessing complexity*, Basic Books, New York, 2000.
- [4] John Perry Barlow, *A declaration of the independence of cyberspace*, Available at [//www.eff.org/ barlow/library.html](http://www.eff.org/barlow/library.html), 1996.
- [5] Franz Brentano, *Von der klassifikation der psychischen phnomene (psychologie ii)*, Meiner, Hamburg, 1912 [1971].
- [6] Manuel Castells, *The rise of the network society*, Oxford University Press, Oxford, 2000.
- [7] ———, *The internet galaxy*, Oxford University Press, Oxford, 2001.
- [8] Francesco Galgano, *Storia del diritto commerciale*, Il Mulino, Bologna, 1980.
- [9] Herbert L. A. Hart, *The concept of law*, Oxford University Press, Oxford, 1961.
- [10] Thomas Hobbes, *Leviathan*, Penguin, London, [1651] 1968.
- [11] David Hume, *Enquiries concerning human understanding and concerning the principles of morals*, Clarendon, Oxford, 1975.

- [12] Will Hutton and Anthony Giddens, *On the edge. living with global capitalism*, Vintale, London, 2001.
- [13] Lawrence Lessig, *Code and other laws of cyberspace*, Basic Books, New York, 1999.
- [14] ———, *The law of the horse: What cyberlaw might teach*, Harvard Law Review **113** (1999), 501–546.
- [15] David K. Lewis, *Conventions: A philosophical study*, Harvard University Press, Cambridge (Mass), 1969.
- [16] Peter Ludlow, *Crypto anarchy, cyberstates, and pirate utopias*, MIT, Cambridge (Mass), 2001.
- [17] John Naughton, *A brief history of the future. the origins of the internet*, Orion, London, 2000.
- [18] Robert Nozick, *Anarchy, state and utopia*, Blackwell, Oxford, 1974.
- [19] Enrico Pattaro, *Filosofia del diritto*, Clueb, Bologna, 1998.
- [20] John Rawls, *Political liberalism*, Columbia University Press, New York, 1993.
- [21] Joel R. Reidenberg, *Lex informatica: The formulation of information policy rules through technology*, The Philosophical Review **76 (3)** (1996), 553–584.
- [22] Jeremy Rifkin, *The age of access*, Penguin, London, 2000.
- [23] Thomas Schelling, *The strategy of conflict*, Oxford University Press, Oxford, 1960.
- [24] Edna Ullman-Margalit, *The emergence of norms*, Clarendon, Oxford, 1977.