

Stefano Rodotà

Ethics and Human Rights in the Information Society

Today's information society looks like a battlefield, where hard law and soft law, ethics and law are continuously at variance. Multiple stakeholders, conflicting interests, and the irreducibility to the domestic dimension make it difficult – at times impossible – to regulate with the help of conventional tools such as domestic laws or international conventions. These factual difficulties are compounded by conceptual analysis, whereby self-regulation is said to be preferable over rules imposed from the outside because such rules are allegedly regarded as authoritarian – at the very least, paternalistic. In fact, Internet is supposedly in need of no binding rules; indeed, rules might affect the intrinsically libertarian nature of the Internet. Thus, soft law is regarded from different quarters as the most suitable tool to regulate the ever-changing, mobile, diffuse, or downright elusive information society.

Starting from these considerations, the focus has been shifting stepwise towards tools that are termed in different ways – codes of conduct, codes of ethics, codes of good practice, netiquette, blotiquette, and so on. Though retaining the word “code” – which is a tribute paid to the legal dimension – these instruments are actually putting emphasis on ethics. The underlying reasons are obvious. Ethics is highly evocative as a word; it points to the existence of values and hints to the responsibilities vested in the individual stakeholders. Ethics is therefore considered a necessary tool to remedy the real or alleged difficulties encountered by law. Codes of ethics have been spawned in the most diverse sectors and feature, at times, considerable ambiguities. Indeed, some of them are ultimately little more than proclaims devoid of concrete effects and are only used to convey a reassuring image of the organisations that have drafted them.

Still, the nature of codes of conduct / codes of ethics has also undergone some changes. Influential institutions, both national and international – including Unesco – have adopted codes that take on *moral* authority and can work as reference models for public and private entities. Special significance should be attached, for instance, to article 27 of European directive 95/46 on the protection of personal data. This article envisages specific mechanisms and procedures to draft and adopt codes of conduct at both Community and domestic level, with the contribution of national data protection authorities as well as the Working Party set up under article 29 of the Directive. The latter bodies are in charge of checking that the draft codes are compliant with both the directive and national implementing legislation; after their adoption, the European Commission “may ensure appropriate publicity” for them. There is little doubt that such codes do not merely mirror the self-regulation of a given industry; in fact, they are the end-product of the collaboration between public and private entities – so much so that in some legal systems (e.g. in Italy) the adoption procedure may lead the codes of conduct to ultimately become part of the sources of law. This means that soft law can become hard law, that there is a shift from ethics to law – as per the title of a bio-ethics report prepared by the French Conseil d'Etat – and national authorities are additionally in charge of “ensuring” not only their dissemination, but also “*compliance*” with their provisions (as per section 12 of Italy's personal data protection Act).

This evolution is grounded on multifarious reasons – but all of them are basically related to the circumstance that it is increasingly necessary, in today's information society, to safeguard the fundamental rights of individuals. To that end, setting out rules is increasingly perceived as indispensable: although such rules cannot be as binding as laws, they prevent safeguards from being committed exclusively to self-regulation, or the action and responsibility of entities that might also be ready to restrict or violate those rights. This is why the new generation codes of conduct arise out of the need to meet those requirements – as has been recognised in an especially clear-cut manner by article 8 of the EU's Charter of Fundamental Rights, where data protection is enshrined as a fundamental right of the individual. Thus, one is faced ultimately with the issue of how to build up

a *constitutional* dimension for the protection of fundamental rights in the information society. In this perspective, codes of conduct cannot play a central role, also because in too many cases they express mainly corporate interests.

How can we go beyond this logic? In the last times reference has been made to an Internet Bill of Rights, to a “constitution” for Internet. The need for this kind of document may not be challenged by emphasizing the intrinsically libertarian nature of the Net – which would be allegedly endangered by rules. There have been several instances of late in which Internet users’ rights have been infringed – reference can be made, in particular, to the censorship initiatives undertaken by the Chinese government and the collaboration provided by Microsoft and Yahoo!. This has shown that safeguarding network freedoms should not be left to the network’s self-correction capabilities. Microsoft has agreed to warn their Chinese users against using words such as “freedom”, “democracy” or “participation” in their electronic messages. Yahoo! has made available the information required to trace the email sent by a journalist – Shi Tao – to the US, in which he reported on a notice sent to journalists by the Chinese government to inform about the dangers related to the possible presence of dissidents on the occasion of the anniversary of Tienanmen Square events. Shi Tao was subsequently sentenced to ten years’ imprisonment on account of having disclosed confidential information. But it is not just in China that Internet freedom is in danger. If no framework of institutional safeguards is in place, rules are only produced by authoritarian regimes, or else developed by the marketplace – which is not above sacrificing citizens’ rights.

Moreover, major companies such as Microsoft, Google, Yahoo! and Vodafone have announced that a “Charter” is to be issued by the end of this year with a view to protecting freedom of speech on the Internet. Parliaments should not accept that free speech safeguards – which the US decided to enshrine in the First Amendment to their Constitution – become the province of private entities, who will undoubtedly only provide those safeguards that fit in with their interests.

Internet is the largest public space ever known to mankind. Every single day there are millions of people that use the Internet to exchange messages, produce and receive knowledge, build up their participation in political and social events, play, purchase, exchange goods and services. Should all this be relinquished to make way for the prevarication of authoritarian regimes, or else market interests?

It is the force of events that is overcoming the resistance of those who stubbornly reject the very concept of an Internet Bill of Rights – because they are afraid that by so doing one might impose constraints that are incompatible with the network’s libertarian history. But this is a backwater stance. It does not take account of reality – where there is day by day a growing number of situations in which network rights are jeopardized, not only by authoritarian regimes but in Western countries as well. Indeed, the argument of countering terrorism is used to mandate long data retention periods with regard to all manners of electronic communication, the delivery of sensitive information to law enforcement bodies or the creation of databases including records on millions of individuals. Nor does this view take into account that constitutions, charters and bills of rights have never placed constraints on freedom – in fact, they have worked as tools to allow safeguarding and enhancing rights.

This does not mean that one should go the same way as that followed in the past to achieve the enactment of constitutional charters and bills of rights. These have been typically handed down – whether as “octroyées” constitutions, i.e. granted by the sovereign, or as instruments adopted by constitutional assemblies. The very nature of the Internet goes against the grain of this approach. Internet is the place of public discussion, of the initiatives that are intended to and can involve a huge number of individuals – it is a forum for working co-operatively. This is where the criticisms mentioned above make sense – it is not as if someone might imagine that an Internet Bill of Rights could be developed by following the process that is typically implemented for international conventions, where sherpas from foreign ministries prepare a draft for submission to the UN

General Assembly. What is required here is shifting from a top-down to a bottom-up approach: from merely approving a draft to building up shared rules.

An Internet Bill of Rights is bound to be the outcome of a process, the end-product of the initiatives undertaken by the “dynamic coalitions” already working on the Net – which have paved the way to a veritably global debate. This is no wishful thinking – indeed, a time-schedule and control mechanisms can be developed for this process, thanks to the annual meetings of the UN Internet Governance Forum (the next one being held in November 2007 in Rio de Janeiro). This is going to be a lengthy process fraught with several difficulties. However, one does not need to await its conclusion to be rewarded with some results. There is room for intermediate steps; partial agreements; declarations applying to world regions and/or specific sectors. There are actually examples and proposals already at hand. The most articulate system of personal data protection can be found in the European Union, and important guidelines can be derived from this experience in view of drafting an Internet Bill of Rights.

One should go beyond the traditional framework of international conventions. It is necessary to complement that framework by instruments that enable a number of societal stakeholders to prick up their ears and contribute – so as to achieve a really multi-stakeholder approach involving all the parties concerned. Taking the cue from the definition of the Internet as the “network of networks”, one might meanwhile develop a “framework of existing framework principles” – for instance by taking advantage of the experience gathered via the available codes of ethics.

The issues arising at this point are twofold – what contents should be included in an Internet Bill of Rights, and how the protection of human rights in knowledge society can reach beyond the boundaries of the Net. These two issues are actually mutually related. Some rights and freedoms should be affirmed as part and parcel of the new world-wide citizenship. The freedom to access knowledge must be recognised in a knowledge society – which entails not only the possibility to connect, but also the need to increasingly regard the goods available on the Net as common property. Free speech should consist not only in rejecting all new forms of censorship, but also in recognising the right to anonymity and the full freedom to “seek, receive and impart information and ideas” (as per article 19 of the Universal Declaration of Human Rights). Considering the protection of personal data as an autonomous fundamental right – other than the conventional right to privacy – is an essential component of contemporary freedom; indeed, it is indispensable to rebut the vision of knowledge society entertained in some circles, whereby public and private entities are allegedly empowered to become apprised of every single item of information concerning individuals. If this were the case, democratic societies would be turned into societies resting on control, surveillance, classification and social selection. Here is where one has to tackle the issue of how and to what extent information may be collected, given that data collection is increasingly based on data retention and the availability of all types of electronic communication; the growing use of video surveillance and similar techniques; invasive applications of biometrics and genetics; and the modifications brought about in the human body as such via technologies (such as Rfid) that allow unrelenting location and surveillance.

Ethical standards and legal principles should converge on setting out the framework safeguards required to prevent a highly dangerous type of social, political, and institutional schizophrenia. Highly ambitious instruments such as the Eu’s Charter of Fundamental Rights have brought about the constitutionalisation of the person – starting from personal freedom and dignity. Still, the principles affirmed in such instruments are continuously breached by political, social and legal practices that reduce or do away with safeguards to meet the requirements made by domestic or international security and/or market interests. In the past, in the Magna Charta, the *habeas corpus* consisted in the promise made by the king to his knights that they would not be imprisoned or tortured illegally – “nor will go upon him nor send upon him.” This promise should be renewed and shifted from the physical body to the electronic body – i.e. to the individual living in a globalised world, whose information is a fundamental component of knowledge society.

The inviolability of the person in the electronic dimension makes it necessary to afford everyone the right to freely develop their own personalities – which postulates, in turn, not only putting in place safeguards against breaches of the private sphere and recognising full rights in terms of access to knowledge, but also the rejection of all kinds of reductionism. Unesco’s Universal Declaration on the Human Genome and Human Rights states that “dignity makes it imperative not to reduce individuals to their genetic characteristics” (article 2b.). The same applies to information. We should not be reduced to our data, and every person has the right not to be simplified, objectified, and evaluated out of context. Between ethics and law, the public projection of our *persona* – the manner in which we are perceived by the others in the information society – attains to a right to identity, and this right must become the focus of laws and codes of conduct, of both hard and soft law.