Ethics Inf Technol (2012) 14:319–328
DOI 10.1007/s10676-012-9295-9

ORIGINAL PAPER

Cracking down on autonomy: three challenges to design in IT Law

U. Pagallo

Published online: 8 June 2012

Abstract The paper examines how technology challenges conventional borders of national legal systems, as shown by cases that scholars address as a part of their everyday work in the fields of information technology (IT)-Law, i.e., computer crimes, data protection, digital copyright, and so forth. Information on the internet has in fact a ubiquitous nature that transcends political borders and questions the notion of the law as made of commands enforced through physical sanctions. Whereas many of today's impasses on jurisdiction, international conflicts of law and diverging interpretations of statutes can be addressed by embedding legal safeguards in ICT and other kinds of technology, to overcome the ineffectiveness of state action by design entails its own risks, e.g., threats of paternalism hinging on the regulatory tools of technology. Rather than modelling people's behaviour by design, the article suggests that design policies should respect individual and collective autonomy by decreasing the impact of harm-generating behaviour (e.g., security measures and default settings for data protection), or by widening the range of people's choices (e.g., user friendly interfaces).

Keywords Autonomy · Data protection · Design · Digital rights management · Information technology Law · Jurisdiction · Paternalism · Privacy by design · Self-enforcement technologies

U. Pagallo (✉)
Law School, University of Turin, via s. Ottavio 54, 10124 Turin, Italy
e-mail: ugo.pagallo@unito.it

Introduction

In *Ethical Aspects of Autonomous Systems*, Herman Tavani has recently stressed the difficulty to define the concept of "autonomy" (Tavani, in press). Some equate it with such different notions as privacy, voluntariness, and free choice (Faden and Beauchamp 1986). Others link the concept to liberty, dignity, responsibility, and self-knowledge of one's interests (Dworkin 1988). Besides, over the past years, scholars have debated whether artificial agents can be autonomous as George Bekey claims in *Autonomous Robots* (2005). Following the criteria singled out by Floridi and Sanders (2004), we could properly talk about autonomous artificial agents (AAs), in that AAs: (1) respond to stimuli by changing the values of their inner states, (2) are capable of modifying these states without external stimuli, and (3) can improve the rules through which these states change. Some scholars claim, however, that this view is inadequate, since AAs do not meet the necessary and sufficient conditions required for autonomous behaviour such as consciousness, free will and intentionality (Himma 2009). In light of this debate, the article proposes a stricter view of autonomy, by adopting Kant's classical definition of "the property that the will has of being a law to itself" (Kant 1795).

This definition, to be sure, has been criticized throughout the past two centuries, that is, from Hegel's remarks on how Kant's concept of autonomy could not ground any particular substantive value commitment, down to recent findings of neuroscience and cognitive psychology, according to which the idea of being sovereigns of our own self would be self delusional. This is why, for instance, Judith Butler suggests we have to focus on the cognitive, social, and institutional conditions under which a reasonable account of people's autonomy can be given (Butler

2005). Likewise, Mireille Hildebrandt proposes that we should "try to come to terms with the idea of autonomous action as the hallmark of human freedom, safely rooted in a constitutive opacity that grounds the self in the abyss of its own inaccessible beginnings" (Hildebrandt 2011). Although other scholars similarly propose to downplay Kant's transcendental version of autonomy as well as the pure cognitive features of practical reason, I insist on Kant's definition on the property that the will has to literally rule (*nomos*) over itself (*auto*), to stress how the information revolution currently affects some legal and political corollaries of such viewpoint.

The first corollary has to do with the idea of collective autonomy and the right of the states to control events within their territory in the name of the principle of sovereignty. Here, "autonomy" is related to the independence of every member of a commonwealth as a co-legislator of the laws. According to Kant's phrasing, the sovereign should "give his laws in such a way that they could have arisen from the united will of a whole people and to regard each subject, insofar as he wants to be a citizen, as if he has joined in voting for such a will" (Kant 1795).

The second corollary concerns the idea of individual autonomy as "the independence from being constrained by another's choice" (*ibid*). Although Kant does not endorse any democratic claim, this second form of independence stands against every sort of paternalism, in that citizens should never be treated as if they were unable to understand what is harmful or useful to them.

Finally, from the legal and political idea of autonomy (both individual and collective) it follows a basic tenet of the rule of law such as the principle of *habeas corpus*. In a nutshell, the idea is that people should be protected against every kind of arbitrary (public and private) action and, moreover, they have to have a say in the decisions affecting them.

Whether collective, individual, or entwined with the traditional principle of *habeas corpus*, today's information revolution challenges such legal and political corollaries of the "property that the will has of being a law to itself." The ubiquitous nature of information on the internet transcends conventional boundaries of national legal systems, as shown by cases that scholars address as a part of their everyday work in the fields of information technology (IT)-Law, i.e., data protection, computer crimes, digital copyright, e-commerce, and so forth. *Pace* the hyper-activism of lawmakers, at both national and international levels, the traditional idea of the law as a set of rules enforced through the menace of physical sanctions (e.g., Kelsen 1949) often falls short in coping with cases of spamming, phishing, or identity thefts. In the field of intellectual property law, for example, the European legislators have enacted the directives D-2001/29/EC, D-2001/84/EC, D-2004/48/EC, D-2006/115/EC, and D-2006/116/EC. However, in the 2010 Report on the application of the EU copyright directives, the European Commission concedes that "despite an overall improvement of enforcement procedures, the sheer volume and financial value of IP rights infringements are alarming" (SEC-2010-1589 final).

Meanwhile, threats and risks on the internet have suggested private companies and hundred millions people alike to opt for more reliable, yet sterile applications. Besides e-books, mobile phones, or video games consoles, Facebook's closed e-mail system or Apple's model of services and mobile devices are creating a set of digital walls. Furthermore, consider the ways some Western democracies and authoritarian regimes alike have specified the functions of state action on the internet. Some countries, as France or South Korea, have endorsed the so-called "three strikes"-doctrine, as a part of the graduated system which ends up with the user internet disconnection after three warnings of allegedly copyright infringements. Other states, like China, have built up systems of filters and re-routers, detours and dead-ends, to keep internet users on the state-approved online path. Whilst, in December 2010, some members of the EU Commission similarly proposed to adopt a system of filters in order to control the flow of information on the internet, there are risks of paternalism as well, insofar as the aim of some lawmakers is to protect citizens even against themselves. In light of Kant's definition of autonomy, as opposed to every form of paternalism, it is thus crucial to understand the further reasons why some legal and political corollaries of the rule of law and people's "property of being law to themselves" are often cracked down in the new environment. Aside from the technological skills of authoritarian regimes, e.g., China's "Great Firewall," the paper suggests we should pay attention to three challenges of the current information revolution in the Western world.

Next, I insist on limits of the traditional viewpoint that conceives the law as a set of rules enforced through physical sanctions in a context where physical borders are increasingly irrelevant: *the first challenge* of the information revolution concerns the difficulty of traditional state action to preserve people's rights and whether this problem can be addressed by embedding legal safeguards into technology. In "Enforcement by design," I dwell on the ways lawmakers and private companies have dealt with the new scenarios of the information revolution through design, codes, and IT architectures: in light of the use of self-enforcement technologies, such as digital rights management (DRM) and some versions of the principle of "privacy by design," *the second challenge* of the information revolution has to do with the ethical stakes of the aim to embed legal safeguards into technology. In "The legal stakes of design," the focus is on the different goals

design may have. By distinguishing between the aim to decrease the impact of harmful behaviour and the task to prevent social behaviour from occurring, *the third challenge* of the information revolution regards the overcoming of the inefficacy of traditional state action in digital environments, yet averting threats of paternalism that hinge on the regulatory tools of technology. In "Changing behaviour," I propose a stricter approach to design mechanisms so as to properly complement the traditional version of the principle of *habeas corpus* with a new kind of protection for people's online interaction. Many of today's troubles with jurisdiction, international conflicts of law and diverging interpretations of statutes can be tackled by applying design properly if, and only if, such design policies respect individual and collective autonomy. In accordance with the Kantian property of the will to be law to itself, let us examine how this "win–win" scenario is possible.

Law on the internet

Technology challenges the conventional national boundaries of contemporary legal systems, in that information on the internet has a ubiquitous nature that transcends political borders and calls into question the notion of the law as made of commands enforced through physical sanctions. While virtually all events and transactions have "border-crossing effects" in the new environment (Post 2002), citizens of nation states are often affected by conduct that the state is unable to regulate (e.g., spamming). Remarkably, since the mid 1990s, scholars have addressed the new generation of IT-cases as computer crimes, digital copyright, data protection, and more, with the settled principles and traditional tools of international law. Jack Goldsmith's remarks in *Against Cybernarchy* (1998) make the point clear: IT law-cases would be "no more complex and challenging than similar issues presented by increasingly prevalent real-space events such as airplane crashes, mass torts, multistate insurance coverage, or multinational commercial transactions, all of which form the bread and butter of modern conflict of law" (*op. cit.*). Yet, spamming is a good example of the troubles of state-action, because spamming is *par excellence* a transnational business that, although illegal, does not diminish despite harsh criminal laws (as the *CAN-SPAM Act* approved by the US Congress in 2003). According to David Post's criticisms of the idea that "activity in cyberspace is functionally identical to transnational activity mediated by other means, such as mail or telephone or smoke signal" (Goldsmith 1998), we should pay attention to a peculiarity of cyberspace: the extraterritorial effects of people's behaviour that were the exception in all the previous legal frameworks of both private and public international law, represent today's "core of that system." Like in other fields of scientific research such as physics, biology, or engineering, scale matters: "A world in which virtually *all* events and transactions have border-crossing effects is surely not 'functionally identical' to a world in which most do not, at least not with respect to the application of a principle that necessarily requires consideration of the distribution of those effects" (Post 2002).

The ubiquitous information of the internet has not only magnified the troubles with the enforcement of the law in the new environment, but it has led to the illegitimate condition where states claim to unilaterally regulate extraterritorial conduct by imposing norms on individuals who have no say in the decisions affecting them (therefore jeopardizing another tenet of the democratic rule of law). For example, in the Document on the application of EU data protection law, the European privacy commissioners, i.e., the Working Party art. 29 argue that even when a "US web site puts a cookie on the personal computer of individuals in the EU in order to identify the PC to the web site in view of linking up that information with others," EU law should be applicable (WP29 2002). In accordance with the thesis on the principle of sovereignty and "a nation's right to control events within its territory" (Goldsmith 1998), the WP29 claims that "a survey of international law suggests that States have a tendency to use several alternative criteria for determining extensively the scope of application of national law" (WP29 2002). However, the European privacy commissioners also affirm that the aim to applying a traditional principle of international law such as "territoriality" is legitimated by the protection of individual rights: "The objective of this provision in Article 4 paragraph 1 lit. c) of Directive 95/46/EC is that an individual should not be without protection as regards processing taking place within his country, solely because the controller is not established on Community territory. This could be simply, because the controller has, in principle, nothing to do with the Community. But it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law" (§ 2 of the Document).

Some scholars have of course insisted on some inconsistencies of this conclusion (Kuner 2003). After all, the WP29's thesis would end up in a paradox once you admit that cookies in your PC do represent 'equipment' pursuant to art. 4(1)-c of the European directive on data protection (D-95/46/EC). When a US citizen is accessing a US web site during, say, our next meeting in Italy, it would follow that the enforceable norms are the EU laws on data protection, so as to determine, for example, whether we are dealing with "personal data" at all! More convincingly, in the Opinion from July 25th, 2007, the European data

protection supervisor, Peter Hustinx, calls for further international agreements. By recalling the decision of the European Court of Justice in the Lindqvist case (C-101/01), Hustinx argues that "this system, a logical and necessary consequence of the territorial limitations of the European Union, will not provide full protection to the European data subject in a networked society where physical borders lose importance (…): the information on the Internet has an ubiquitous nature, but the jurisdiction of the European legislator is not ubiquitous" (Hustinx 2007).

The difficulty of state action to protect a basic tenet of the rule of law such as the principle of *habeas corpus*, has suggested lawmakers (and private companies) to increasingly adopt a number of technological measures, such as codes (Lessig 1999), architecture (Katyal 2003), and design (Yeung 2007). Although these measures are not necessarily digital, e.g., the installation of speed bumps in roads as a means to reduce the velocity of cars, the information revolution has obliged lawmakers to forge more sophisticated ways to think of legal enforcement. This is the case of data protection, where design should aim to ensure the minimization and quality of the data, its controllability, transparency, and confidentiality. Likewise, in the field of copyright and intellectual property, self-enforcement technologies as digital right management (DRM)-devices aim to enable right-holders to monitor and regulate the use of their copyright protected works. As a solution to conflicts concerning jurisdiction and law enforcement in digital environments, that is, the first challenge of the information revolution, private companies as well as governments have therefore leaned all the more on the regulatory tools of technology, so as to tackle the difficulties of state action to protect people's rights in the new environment. Let me examine, in the next section, a first example of this kind of legal "enforcement by design."

Enforcement by design

Since the mid 1990s, companies and big business have tried to find a remedy for the troubles of state action to protect their interests on the internet. In the field of copyright and intellectual property, for example, most of the efforts focused on how to safeguard such exclusivity rights through the development of self-enforcement technologies as DRM. By enabling right-holders to strictly regulate the use of their own copyright protected works, companies would have prevented unsolvable problems concerning both the enforceability of national norms and the conflicts of law at the international level. Whereas, in his *Thoughts on Music* (2007), Steve Jobs conceded that DRM compliant systems raise severe challenges of interoperability and, hence, antitrust issues, the use of DRM techniques ultimately impinges on people's right to have a say in the decisions affecting them, because a kind of infallible self-enforcement technology collapses "the public understanding of law with its application eliminating a useful interface between the law's terms and its application" (Zittrain 2007). Furthermore, as a response to the limits of state-action, the use of DRM technology risks to severely curtail individual freedom and collective autonomy, since people's behaviour would unilaterally be determined on the basis of technology, rather than by choices of the relevant political institutions.

Still, lawmakers have proposed and, sometimes, requested private companies to employ technical and organizational measures in order to guarantee the enforcement of the law. As mentioned in the introduction, the European Commission's 2010 Report on the EU copyright directive, that is, D-2004/48/EC, affirms that "the sheer volume and financial value of IP rights infringements are alarming. One reason is the unprecedented increase in opportunities to infringe IP rights offered by the internet" (SEC-2010-1589 final). In order to stop such illegal activities, the European Commission is currently examining the legitimacy of "a system for filtering all electronic communications" and, especially, peer-to-peer (P2P) applications. Besides, the EU Commission is supporting a new generation of injunctions that should be taken against the internet service providers (ISPs), regardless of their liability, with the goal to prevent "further infringements" even in the event of extra-territorial effects. Leaving aside whether or not we should amend today's clauses of responsibility for ISPs, such as Article 15 of the EU directive on e-commerce (D-2000/31/EC), it follows that the second challenge to design in IT law concerns the ethical stakes of embedding legal safeguards into technology. At the end of the day, would it be morally acceptable to embrace the idea of the Ontario's Privacy Commissioner, according to whom personal data should be automatically protected in every IT system as its default setting, so that a cradle-to-grave, start-to-finish, or end-to-end lifecycle protection would ensure that privacy safeguards are at work even before a single bit of information has been collected? (Cavoukian 2010) Would self-enforcement technologies be a legitimate way to complement the traditional principle of *habeas corpus*, linked to the physical body of each individual, with a new kind of protection against arbitrary actions to people's "electronic body"?

All in all, there are two reasons why such an approach to design mechanisms seems highly controversial: on one hand, there is evidence that "some technical artefacts bear directly and systematically on the realization, or suppression, of particular configurations of social, ethical, and political values" (Flanagan et al. 2008). While specific design choices may result in conflicts between values, vice versa, conflicts between values may impact on the features of design. Even though legal systems help us overcome a

number of conflicts between values (Flanagan et al. 2008), it is likely that the use of self-enforcement technologies in fields as data protection would make conflicts between values even worse, due to specific design choices, e.g., the opt-in versus opt-out diatribe over the setting for users of information systems. On the other hand, design approaches to privacy as "automatic control" appear even more problematic than the use of DRM technology for the protection and enforcement of digital copyright, because data protection does not represent any automatic "zero-sum game" between options of access and control over information in digital environments. Personal choices play in fact the main role when individuals modulate different levels of such access and control, depending on the context and its circumstances (Nissenbaum 2004). In addition, there is the technical difficulty of applying to a machine concepts traditionally employed by lawyers, through the formalization of norms, rights, or duties: as a matter of fact, informational protection safeguards present highly context-dependent notions as personal data, security measures and data controllers, that raise a number of relevant problems when reducing the informational complexity of a legal system where concepts and relations are subject to evolution (Pagallo 2010). Not only issues of jurisdiction considered in the previous section can hardly be reduced to a software engineering-debate, but 10 *years of efforts* on platforms for privacy preferences show that, say, "the P3P specification is not yet mature enough in terms of element definitions to handle many legal subtleties cleanly" (Jutla 2010). To the best of my knowledge, it is impossible to program software so as to prevent forms of harm generating-behaviour even in such simple cases as defamations: these constraints emphasize critical facets of design that lie behind the use of allegedly perfect self-enforcement technologies. Consider three aspects of the problem:

First, there is the risk of updating traditional forms of paternalism, in that people's behaviour would unilaterally be determined on the basis of automatic techniques, rather than by individual choices on levels of access and control over information: "the controls over access to content will not be controls that are ratified by courts; the controls over access to content will be controls that are coded by programmers" (Lessig 2004).

Second, attention should be drawn to the difficulties of achieving such total control. Doubts cast by "a rich body of scholarship concerning the theory and practice of 'traditional' rule-based regulation bear witness of the impossibility of designing regulatory standards in the form of legal rules that will hit their target with perfect accuracy" (Yeung 2007).

Third, in the case of data protection, we should stress the problems of embedding privacy safeguards into technology, for people may enjoy privacy in the midst of a crowd and without having total control over their personal data, whereas total control over that data does not necessarily entail any guarantee of privacy (Tavani 2007).

Accordingly, after the troubles of state action with the protection of people's autonomy on the internet (challenge 1), and the ethical problems raised by the prospect of embedding legal safeguards into technology (challenge 2), the next section introduces the third challenge to design in IT law. Let me focus on the feasibility to overcome the ineffectiveness of state action in digital environments, averting threats of paternalism that hinge on the regulatory tools of technology.

The legal stakes of design

The information revolution has affected Kant's legal and political corollaries of the idea of autonomy, namely, his version of the rule of law (*Rechtsstaat*) and the principle of *habeas corpus*: the property that the will has to be law to itself is currently entwined with the multiple ways we determine the form of products and processes, as well as the structure of spaces and places, so as to comply with regulatory frameworks. The impact of design on both social relationships and the functioning of legal systems involves a number of relevant issues such as privacy and universal usability, informed consent and crime control, social justice and reputation schemes. From a legal point of view, what is at stake here mainly concerns whether some kinds of design mechanisms violate people's right to have a say in the decisions affecting them, that is, what the German Constitutional Court has framed in terms of people's "informational self-determination," since its *Volkszählungs-Urteil* ("census decision") from 15 December 1983. As well known, both Article 8 of the EU Charter of Fundamental Rights and the EU directive 46 from 1995 aim to complement the traditional version of the principle of *habeas corpus* (Bingham 2011), with a new kind of protection for people's "informational self-determination." Among the criteria for making data processing legitimate, we find cases where individuals have the right to determine whether personal data can be collected and, eventually, transmitted to others; the right to determine how the data may be used and processed; the right to access that data and, where necessary, to keep it up to date; down to the right to delete that data and to refuse at any time to have the data processed. All the provisions concerning, say, the aforementioned directives on copyright and intellectual property (D-2004/48/EC), or e-commerce (D-2000/31/EC), should be considered in light of this "electronic autonomy." In the wording of D-2003/98/EC on the re-use of the public sector information, such directives "should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC."

However, there are many ways in which the design of products and processes, along with the form of spaces and places, may impinge on people's "informational self-determination." In their work on *The Design with Intent Method* (2010), for instance, Lockton, Harrison and Stanton describe 101 ways in which products can influence the behaviour of their users. In this context, it suffices to stress three different ways design affects today's legal provisions on people's autonomy. Besides mechanisms that prevent social behaviour from occurring via the use of allegedly self-enforcement technologies (see previous section), consider the legitimacy of design mechanisms that aim to decrease the impact of harmful conducts or, alternatively, to encourage the change of people's behaviour. As an illustration of this latter aim of design, i.e., the change of people's conduct, consider Facebook's issues with data protection laws as confirmed on 26 May 2010. On that occasion, the social network announced to have "drastically simplified and improved its privacy controls" which previously amounted to 170 different options under 50 data protection-related settings. Likewise, reflect on the free-riding phenomenon of P2P networks, where most peers tend to use these systems to find information and download their favourite files without contributing to the performance of the system. Although this selfish behaviour is triggered by many properties of P2P applications like anonymity and hard traceability of the nodes, designers have proposed ways to tackle the issue through incentives based both on trust (e.g., reputation mechanisms), and trade (e.g., services in return). Whether dealing with a client–server architecture such as Facebook's or a P2P "servent" system, that is, nodes of the network that are clients and servers at the same time, what these examples are suggesting is to focus on a specific aim of design policies. Rather than self-enforcement technologies and automatic systems for filtering all electronic communications, such as those examined by the EU Commission in the 2010 Report on the copyright directive, design may encourage people's change of conduct as we do with modifications to user interfaces by increasing, or reducing, the prominence of a default setting, so as to allow individuals to configure and use their software as they deem appropriate. Despite different definitions of autonomy that scholars endorse in the philosophical domain, this type of design mechanism abides by current legal rules on people's informational self-determination. Here, design choices are legally "neutral" in how they embed values in artefacts, because the aim is to *widen* the range of people's choices.

On the other hand, a new generation of 'digital airbags' can decrease the impact of harm-generating behaviour in the new environment. As an example of such design mechanisms, consider the default configuration of ICT interfaces, so that we can ensure that values of design are appropriate for novice users and, still, the system improves efficiency (Kesan and Shah 2006). Moreover, think of security measures, such as reCAPTCHA, that aim to prevent automated programs from abusing online services (von Ahn et al. 2008). The purpose of such design policies looks morally and legally sound, because their function is similar to traditional airbags for cars that increase people's security. Let me mention three aspects of the parallelism:

First, digital airbags do not impact on individual conduct and ways, say, people interact on digital highways, lest traditional airbags suggest people to drive their cars even more safely.

Second, by embedding data protection safeguards in ICT or designing spaces, processes and products, this sort of 'digital airbags' look particularly fruitful because the aim is to decrease the informational entropy of the "infosphere" (Floridi 2003); that is, the impoverishment of the new environment and its informational objects through forms of spamming, phishing, identity thefts, automated programs for abusing online services, and the like.

Third, such a stricter approach to design policies prevents multiplying conflicts of values with their divergent interpretations through design choices, because these choices mostly concern the technical meticulousness of the project or the impact of technical inaccuracies on individual well-being, rather than people's values and autonomous decisions. A typical instance is given by the processing of personal data in hospitals via information systems, whereas patient names should be kept separated from data on medical treatments or health status. Developers of such information systems do not have to determine whether the processing of personal data is legitimate or what kind of data should be conceived of as personal. Focus is on the functional efficiency, robustness, reliability, and usability of the design project, so that, through the use of prototypes, internal checks among the design team, users tests in controlled environments, surveys, interviews, and more, "verifying the inclusion of values is likely to draw on strategies and methods not unlike those applied to other design criteria like functional efficiency and usability" (Flanagan et al. 2008). Although the project has to strike a sometimes-difficult balance between the efficacy of the information system and the fact that users, including doctors, may find such mechanism too onerous, the aim is not to change how people behave in hospitals. Rather, the aim is to decrease the impact of harmful behaviour in such environments.

However, how about the third challenge to design in IT law when the aim is to change (rather than encouraging the change of) people's behaviour? As scholars who have been criticizing the European data protection policies (Kuner 2003), and the editorials in *The Economist* often stress,[1]

[1] See the Economist's issue from 6 April 2006 with the special report on "the new paternalism: the avuncular state."

there is a risk that governments would not only guard the citizens' wellbeing against all harms but even against their own will. This modelling people's conduct amounts to paternalism (Kant 1795); and, moreover, it seems to impinge on what the *Bundesverfassungsgericht* has established as the constitutional right to the individual "informational self-determination." Would it be feasible to prevent such threats, when making state action effective in digital environments?

Changing behaviour

In the 2009 Document on "The Future of Privacy," the EU Working Group art. 29 declared that global problems of enforcing people's rights should be addressed by embedding data protection safeguards in ICT, so that the principle of privacy by design should be binding for social network services (WP29 2009b). Ever since the first European directive on data protection, lawmakers have affirmed that their intention was to embed "appropriate measures" in ICT "both at the time of the design of the processing system and at the time of the processing itself" (pursuant to the recital 46 of D-95/46/EC). 15 years later, what European data protection authorities and privacy commissioners are thus suggesting is a stronger responsibility for a specific class of ISPs, such as social network services (SNS), to "advise users" that "pictures or information about other individuals should only be uploaded with the individual's consent" (WP29 2009a). Among the 101 forms in which products can influence the behaviour of their users (Lockton et al. 2010), there are two opposite ways to understand the aim of design to change people's behaviour.

The first way brings us back to the threats of paternalism mentioned in the previous section. Although legal systems help us overcome a relevant number of issues, because designers "need to take into consideration the sometimes detailed guidance of legal doctrine or explicit regulation" (Flanagan et al. 2008), it may be argued that some legal rules can simply be "bad." According to Richard Volkman, for example, the European legal framework "is clearly and deeply flawed as an account of what informational protection is all about" because "restrictions are so sweeping that many perfectly legitimate business models are de facto outlawed by such a law" (Volkman 2003). Correspondingly, we should previously test the goodness of every law in order to prove the goodness of aiming to legally change people's behaviour via technology: projects in security measures illustrate this twofold connection between values and design. Once we are interested in establishing the reliability and technical meticulousness of the project, e.g., security measures in the informative system of a power plant or of hospitals, design seems legitimate since the goal is by definition to decrease the impact of harm-generating behaviour (see previous section). Yet, a lot of problems persist when determining the "harmful" nature of conducts or events design should try to decrease via self-enforcement technologies, e.g., the "alarming" surge of IP infringements that have suggested the EU Commission to examine the legitimacy of "a system for filtering all electronic communications" and, especially, P2P applications (see above in the introduction and "Law on the internet" of this paper).

Luckily, there is a second way to evaluate the aim of design to change people's behaviour. Needless to sympathize with Brussels, to follow the EU Working Party's proposal according to which the principle of privacy by design should be implemented in a bottom-up way, that is, grounded on the autonomous choices of individuals through self-regulation and competition among private organizations through codes of conduct (WP29 2009b). Whereas the goal of ensuring compliance with regulatory frameworks via data protection safeguards in ICT may end up in modelling of individual behaviour, a bottom-up approach prevents this threat by allowing individuals to make their own decisions. This is the case of the aforementioned P2P reputation mechanisms as well as incentives and services in return, e.g., bond schemes that involve forms of digital money like Kazaa's 'Alnet's points.' Rather than directly changing people's behaviour, in other words, design may aim to *encourage* people's change of conduct by *broadening* the range of options available. From this further viewpoint, a stricter approach to design mechanisms seems to be sound because the goal, by definition, is to enrich the flourishing of the "infosphere" and its informational objects (Floridi 2003).

On this basis, we can tackle the third challenge to design in IT law. Whereas the difficulty of the states to protect people's autonomy in digital environments can be addressed by design (challenge n. 1), we should pay attention to the ethical problems of embedding legal safeguards in ICT (challenge n. 2), so as to avert the threat of paternalistic regulators (challenge n. 3). By widening the range of people's choices in the "infosphere," rather than modifying or determining individual conduct through self-enforcement technologies, this purpose of broadening the set of people's options seems as good as the 'digital airbags' that aim to decrease the impact of harm-generating behaviour, e.g., ICT security measures as mentioned in the previous section. While traditional airbags and their digital counterparts do not impinge on individual conduct and how people behave on both traditional and digital highways, additional choices for people's interfaces, user-friendly setting options, or default mechanisms, suggest how to protect rights on the internet by the means of individual autonomy and self-regulation. The duty for ISPs that both

privacy commissioners and lawmakers are putting forward, i.e., to embed legal safeguards into technology by design (WP29 2009b; Cavoukian 2010), goes hand in hand with some of today's "best practices" such as YouTube's users flags, in that companies providing services on the internet encourage people to reflect on what others (and themselves) do online.

Still, even self-regulation, codes of conduct and, generally speaking, a bottom-up approach to design policies have their limits, because the Kantian "property that the will has of being law to itself" ultimately hinges on people's education. As a matter of fact, individuals often ignore what they are doing online when they are, for instance, connected in P2P, namely, becoming servers and clients at the same time. Education will increasingly be required as technology speeds up this profound transformation through the internet of the things, the semantic web, cloud computing and social networks. Some scholars affirm that projects for user control like P3P, PeCAN or HCI-related privacy models, "implicitly have an educational aspect to them" (Jutla 2010). Likewise, public authorities and privacy commissioners often claim that, under certain circumstances, SNS even have a responsibility to "advise" their users (WP29 2009b). Whilst the educational aspects of design are a popular topic of works in design ethics (Grodzinsky et al. 2008; Flanagan et al. 2008; Pagallo 2011a, b), is there a risk of paternalism as a new "avuncular state" by design? What would the educational challenges to design in IT law be?

All in all, there is a substantial convergence between matters of education and the stricter approach to design mechanisms suggested above, because education represents a further reason to be cautious in ensuring compliance with regulatory frameworks through legal safeguards embedded in ICT. Indeed, there is no room for education when design aims to directly change people's conduct or, alternatively, when self-enforcement technologies are employed by legal regulators (lest users reflect upon what they actually are forced to do). Vice versa, design policies may legitimately pursue educational goals if, and only if, their aim is either to decrease the informational impoverishment of the system (e.g., security measures), or to enrich the flourishing of the "infosphere" and its informational objects (e.g., reputation mechanisms). In the first hypothesis, we need no avuncular lawmakers, because education does not consist in directly changing people's conduct but, rather, showing what may occur without such technological devices: think of safety belts for cars and their digital counterparts in ICT systems as procedural constraints for adapting the setting of the interfaces on voluntary and fully informed basis. In the second hypothesis, we prevent every form of paternalism, since design may legitimately aim to encourage the change of individual conduct, when the range of choices available is widened via transparent settings, friendly interfaces and, foremost, values of design that are appropriate even for novice users. Design policies can foster people's education, yet abiding by principles of today's legal framework on people's informational self-determination and the set of rules on how personal data can be collected or transmitted to others, whether such data can be used and processed, whether it should be accessed or deleted, etc. By decreasing the impact of harmful conducts or widening individual options on the internet, these design policies strengthen people's right to education and, still, they avert every claim of paternalism.

Conclusions

The paper has examined some ethical issues emerging with the development and use of information technologies in the field of IT law. Most of today's troubles with jurisdiction and international conflicts of law depend on the twofold features of "generative technologies" like the personal computers and the ways PCs ubiquitously transmit information on the internet. Although they allow innovation, experimentation and the wide-open Web of creative anarchy on the internet, PCs permit the spread of spam, viruses and copyright infringements, that call into question the traditional notion of the law as (1) made of commands; (2) enforced through physical sanctions; (3) within the territory of a sovereign state. Consider the similar case of file-sharing applications like P2P systems: presented by some scholars as the key to a new paradigm in social, political and economic interaction, the EU Commission reckons that P2Ps undermine crucial elements of our societies like incentives for knowledge producers or protection of the exclusive right to exploit the benefit of copyrighted works. Such twofold features of PCs, P2Ps, and other digital means have induced some to present technology as something "neutral," that is, a simple instrument to achieve whatsoever end. Reflect on the further example of *Google Maps*: whereas Brazilian ecologists use such a tool for showing the effects of deforestation in Amazonia, Russian extreme right movement employs the application against immigrants for determining where ethnic minorities live in big cities (Morozov 2011).

The number of ethical issues brought on by the development and application of information technologies, nevertheless, do not simply concern the opposite ways people employ the PCs and some tools as *Google Maps*. Rather, we should conceive technology as a set of constraints and possibilities that transform or reshape the environment of people's interaction. In the case of ICT as with other types of digital technology, this profound transformation is entwined with specific design choices that may result in conflict between values (see above in "Law on the internet"), in

addition to problems of education that suggest we should distinguish between digital natives, naturalized, and new illiterates (see above in "Changing behaviour"). Although people may alternatively use PCs or P2Ps for, say, scientific research or to commit some kind of crime (e.g., identity thefts), we should not miss the broader picture on how such technologies affect social interaction. Some insist on the de-contextuability and re-combinability of content of individual messages (Kallinikos 2006); others present this new scenario as a matter of persistence, replicability, scalability and searchability of information (Boyd 2010). In the case of legal systems, a paramount effect of the ubiquitous nature of online information is that, *pace* the traditional principle of *habeas corpus*, traditional state action often seems incapable to protect people's "property of being law to themselves" in the new environment.

Over the past two decades lawmakers and big business have addressed the first challenge of the information revolution through design, codes, and IT architectures, in such fields as privacy, intellectual property, e-commerce, and so forth. As a matter of fact, technological constraints do not purely delimit the range of possible actions but, according to the seminal remarks of Prigogine and Stengers (1981), "determine in the light of a particular occasion an entire spectrum of intelligible new consequences." Political decisions have attempted to influence, at both national and international levels, the development of technology and how it reshapes or transforms the environment in which people interact, through new statutes on computer crimes, copyright law, data protection, ISP responsibilities, and the like. Yet, information technology has opened new ways for the enforcement of such statutes via allegedly perfect self-enforcement technologies such as DRM, some versions of the principle of "privacy by design," and systems for filtering electronic communications as those examined by the 2010 EU Commission-report on the application of the copyright directive. The second challenge to design in IT law has thus to do with the ethical stakes of embedding legal measures into technology: Would it be feasible to overcome the troubles of traditional state action and preserve people's autonomy on the internet?

The answer depends on the different ways design affects Kant's "property that the will has to be law to itself." In the field of IT law, such "property of the will" is currently framed in terms of people's informational self-determination and the protection of constitutional rights concerning matters of access and control over information in the new environment, e.g., whether personal data can be collected, used, processed, etc. When design mechanisms attempt to directly change individual conduct or automatically prevent social behaviour from occurring, such mechanisms clearly impinge on both individual and collective self-determination (see above in "Enforcement by design"). Conversely, when the aim of design is either to encourage the change of people's behaviour or, alternatively, to decrease the impact of harmful conducts, this stricter approach to design policies looks sound, insofar as the traditional protection of *habeas corpus* is complemented with a new kind of protection for people's "electronic body" (see above in "The legal stakes of design" and "Changing behaviour"). Contrary to the aim of design policies to prevent social behaviour from occurring through self-enforcement technologies, this stricter approach to design may lead to a twofold "win–win" scenario.

On the one hand, by widening the range of the choices available via user-friendly interfaces or transparent setting options, we can strengthen people's right to have a say in the decisions affecting them, in accordance with international covenants and principles of today's legal framework, such as Article 8 of the 2000 European Charter of Fundamental Rights and the principles relating to the protection of personal data established by D-95/46/EC. On the other hand, we can tackle by design the impact of harm-generating behaviour through security measures, default mechanisms and settings for ICT interfaces that, contrary to self-enforcement technologies and massive systems for filtering communications, seem in compliance with a stricter version of the principle of "privacy by design" that both lawmakers (e.g., recital 46 of D-95/46/EC) and commissioners are putting forward (Cavoukian 2010). Accordingly, we can address the final challenge to design in IT law, that is, the menace of treating people as if they were unable to understand what is harmful or useful to them on the internet. Besides "three strikes doctrines" and systems for filtering all electronic communications, think of projects that aim to design a state-approved online path for internet users, such as the *Stop Online Piracy Act* (SOPA) and the *Protect IP Act* (PIPA), which were debated before the US Congress and the Senate in Washington, D.C., between fall 2011 and January 2012. After the Chinese "Great Firewall" and the technological skills of authoritarian regimes mentioned in the introduction, Western countries should not keep internet users on similar paths, automatically enforced through systems of filters and re-routers, detours and dead-ends of the avuncular legislator. Rather than building autonomy from scratch, the aim of Western lawmakers and their design projects for the internet should concern the protection of people's informational self-determination and the enforcement of constitutional rights such as Article 8 of the European Charter. A strict approach to design policies shows how this is feasible in the field of IT law.

References

Bekey, G. A. (2005). *Autonomous robots: From biological inspiration to implementation and control*. Cambridge, Mass: The MIT Press.

Bingham, T. (2011). *The rule of law*. London: Penguin.

Boyd, D. (2010). Social networks sites as networked publics: affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *Networked self: Identity, community, and culture on social networks sites* (pp. 39–58). London: Routledge.

Butler, J. (2005). *Giving an account of oneself*. New York: Fordham University Press.

Cavoukian, A. (2010). Privacy by design: The definitive workshop. *Identity in the Information Society, 3*(2), 247–251.

Dworkin, G. (1988). *The theory and practice of autonomy*. Cambridge, Mass: Cambridge University Press.

Faden, R., & Beauchamp, Th. (1986). *A history and theory of informed consent*. New York: Oxford University Press.

Flanagan, M., Howe, D. C., & Nissenbaum, M. (2008). Embodying values in technology: Theory and practice. In J. van den Hoven & J. Weckert (Eds.), *Information technology and moral philosophy* (pp. 322–353). New York: Cambridge University Press.

Floridi, L. (2003). On the intrinsic value of information objects and the infosphere. *Ethics and Information Technology, 4*, 287–304.

Floridi, L., & Sanders, J. (2004). On the morality of artificial agents. *Minds and Machines, 14*(3), 349–379.

Goldsmith, J. (1998). Against cyberanarchy. *University of Chicago Law Review, 65*(4), 1199–1250.

Grodzinsky, F. S., Miller, K. A., & Wolf, M. J. (2008). The ethics of designing artificial agents. *Ethics and Information Technology, 10*, 115–121.

Hildebrandt, M. (2011) Autonomic and autonomous 'thinking.' Preconditions for criminal accountability. In M. Hildebrandt & A. Rouvroy (Eds.), *The philosophy of law meets the philosophy of technology* (pp. 141–160). Abingdon: Routledge.

Himma, K. (2009). Artificial agency, consciousness, and the criteria for moral agency: What properties must an artificial agent have to be a moral agent? *Ethics and Information Society, 11*(1), 19–29.

Hustinx, P. (2007). Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. *Official Journal of the European Union*, 2007/C 2551/01, July 25th 2007.

Jobs, S. (2007). Thoughts on music. Retrieved at http://www.apple.com/hotnews/thoughtsonmusic/ on September 20th, 2011.

Jutla, D. N. (2010). Layering privacy on operating systems, social networks, and other platforms by design. *Identity in the Information Society, 3*(2), 319–341.

Kallinikos, J. (2006). The consequences of information: institutional implications of technological change. Elgar, Cheltenham, Northampton, Mass.

Kant, I. (1795). Kant's principles of politics, including his essay on perpetual peace. A contribution to political science. (edition 1891) (trans: Hastie W), Edinburgh, Clark.

Katyal, N. (2003). Digital architecture as crime control. *Yale Law Journal, 112*(6), 101–129.

Kelsen, H. (1949). *General theory of the law and the state*. Cambridge, Mass: Harvard University Press.

Kesan, J. P., & Shah, R. C. (2006). Setting software defaults: Perspectives from law, computer science and behavioural economics. *Notre Dame Law Review, 82*, 583–634.

Kuner, Ch. (2003). *European data privacy law and online business*. Oxford, London: Oxford University Press.

Lessig, L. (1999). *Code and other laws of cyberspace*. New York: Basic Books.

Lessig, L. (2004). *Free culture: The nature and future of creativity*. New York: Penguin Press.

Lockton, D., Harrison, D. J., & Stanton, N. A. (2010). The design with intent method: A design tool for influencing user behaviour. *Applied Ergonomics, 41*(3), 382–392.

Morozov, E. (2011). *The net delusion: The dark side of internet freedom*. New York: Public Affairs.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–158.

Pagallo, U. (2010). As law goes by: Topology, ontology, evolution. In P. Casanovas, et al. (Eds.), *AI approaches to the complexity of legal systems* (pp. 12–26). Berlin: Springer.

Pagallo, U. (2011a). Designing data protection safeguards ethically. *Information, 2*(2), 247–265.

Pagallo, U. (2011b). ISPs & rowdy sites before the law: Should we change today's safe harbor clauses? *Philosophy & Technology, 24*(4), 419–436.

Post, D. G. (2002). Against "against cyberanarchy". *Berkeley Technology Law Journal, 17*(4), 1365–1383.

Prigogine, I. & Stengers, I. (1981). Vincolo, *Enciclopedia Einaudi*, 14, 1064–1080. Einaudi, Torino.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy, 38*(1), 1–22.

Tavani, H. T. (in press), Ethical aspects of autonomous systems. In M. Decker & M. Gutmann (eds), *Information- and robot-ethics: Some fundamentals*, Verlag Berlin, Germany.

Volkman, R. (2003). Privacy as life, liberty, property. *Ethics and Information Technology, 5*(4), 199–210.

von Ahn, L., Maurer, B., McMillen, C., Abraham, D., & Blum, M. (2008). reCAPTCHA: Human-based character recognition via web security measures. *Science, 321*(5895), 1465–1468.

WP 29. (2002). EU Working Party art. 29 D-95/46/EC. The international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, WP 56, May 30th 2002.

WP 29. (2009a). EU Working Party art. 29 D-95/46/EC. Online social networking, WP 163, June 12th, 2009.

WP 29. (2009b). EU Working Party art. 29 D-95/46/EC. The future of privacy. WP 168, December 1st 2009.

Yeung, K. (2007). Towards an understanding of regulation by design. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 79–108). London: Hart Publishing.

Zittrain, J. (2007). Perfect enforcement on tomorrow's internet. In R. Brownsword & K. Yeung (Eds.), *Regulating technologies: Legal futures, regulatory frames and technological fixes* (pp. 125–156). London: Hart Publishing.