

*Journal of Information, Communication and Ethics in Society*, Vol. 9 Issue 3, pp. 180-194.  
DOI [10.1108/14779961111167658](https://doi.org/10.1108/14779961111167658)

*This article is © Emerald Group Publishing and permission has been granted for this version to appear on <http://publications.ceu.hu/>. Emerald does not grant permission for this article to be further copied/distributed or hosted elsewhere without the express permission from Emerald Group Publishing Limited.*

The final publication is available at  
<http://www.emeraldinsight.com/journals.htm?articleid=1944204>

## **Regulating the future? Law, ethics, and emerging technologies**

Ivan Szekely, Mate Daniel Szabo and Beatrix Vissy

### **Abstract**

The purpose of the paper is to provide an overview of the legal implications which may be relevant to the ethical aspects of emerging technologies, to explore the existing situation in the area of legal regulation at EU level, and to formulate recommendations for the lawmakers. The analysis is based on the premise that the law is supposed to invoke moral principles. Speculative findings are formulated on the basis of analyzing specific emerging technologies; empirical findings are based on a research conducted in the whole legal corpus of the EU. In the area of network-based technologies the already existing and elaborated legal frameworks can be used in an extended manner; artificial intelligence based technologies call for alterations in several branches of law; while interface technologies show the difficulty and complexity of regulating interdisciplinary fields. The legal implications of emerging technologies have attracted only a minimal legislative attention in the competent bodies of the EU. The paper provides a systemic approach towards transmitting ethical norms to the application of emerging technologies through legal regulation, and formulates detailed recommendations in various areas of such technologies.

**Keywords:** Law, Ethics, Emerging technologies, Network-based technologies, Interface technologies, Artificial intelligence

### **1. Introduction**

Legal implications which may be relevant to the ethical aspects of emerging technologies call out for exploration and discussion. The driving force behind the research presented in this paper was to provide an overview of the areas where law should play an important role in bridging ethical norms and reality in future applications of such technologies. The specific purpose of the research was to formulate recommendations to be implemented in practice by the competent organs of the European Union, thereby influencing the level of

representation of ethical approaches both in research and development of emerging technologies and in the supporting and controlling activities of such organs.

The following analysis is based on the premise that in modern constitutional democracies the law is not simply a matter of rules but is supposed to invoke moral principles (Dworkin, 1996, esp. pp. 1-38; Dyzenhaus et al., 2007, esp. pp. 3-167). These moral principles ought to be expressed in legal rules and institutional solutions, and are supposed to be reflected at national and European level. Such values are also declared in the Preamble of the Charter of Fundamental Rights of the European Union, articulating that "the Union is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity; it is based on the principles of democracy and the rule of law" (European Union, 2000, p. 364/8). Consequently, the starting points of our analysis were the fundamental values as well as principles distilled from these values forming the cornerstones of European (in a broader sense, Western-type) democracies (Smith, 1968, pp. 191 ff.), such as human dignity, equality and the concept of rule of law.

In accordance with the concept that the law incorporates moral values, we do not support the mere *formal* interpretation of the rule of law, which does not contain requirements regarding the *content* of the law. According to our approach – beyond the requirements that the law must be prospective, well-known and unambiguous, and have the characteristics of generality, certainty and predictability – the law is committed to democratic values and intrinsically respects individual rights (Allan, 2003, pp. 23-29). – For more details on the different interpretations of the rule of law, see Tamanaha (2004, esp. pp. 91-113).

## **2. Values and legal systems in the European Union**

Like all other legal systems, the legal systems of European countries cannot be regarded only as the totality of abstract rules either. These rules, both in themselves and as integral components of the various branches of law, are connected with those underlying values, which are decisive factors in the societal relationships and life circumstances of a given country. The closeness of this connection and its visibility vary among countries following different legal traditions: they are stronger in countries following traditions of natural law, and weaker and less direct in countries following a more positivist approach.

The sovereignty of the EU is constituted of national sovereignties, and the common moral/ethical norms can be defined on the basis of such norms of the individual Member States. Still, the common European norms cannot be defined as the "smallest common denominator", nor as an "average" of the Members' ethical or constitutional norms. In addition, the connection is two-directional: the Union is also influencing the law of its Member States both directly and indirectly. It should also be borne in mind that the application of emerging technologies is by no means country-specific, therefore their ethical implications and their demand for legal regulation are not country-specific either.

It should be noted that in the so-called new European democracies the moral value order of society is less stable than that of the societies in traditional democracies, in a certain sense

even less stable than in societies of long-standing dictatorships (Wolchik and Curry, 2008, p. 4; Inglehart and Klingemann, 2003, pp. 174 ff.; Klingemann et al., 2006, pp. 25-66; Howard, 2003, pp. 31-120, 150, and others). Linked with the change of the political system, democratic values, individual freedoms and new hopes to build a more just society were high among the priorities of the members of society, while a few years after the turmoil, such rights and values have become less important (in the area of information rights, see Székely, 2010, p. 166; Zureik et al., 2010). A new generation emerged that valued careers, money, power and other values more than rights, freedom, autonomy, tolerance and the like (Székely, 2007, pp. 120-123). Consequently, when introducing emerging technologies in new democracies, the legal guarantees of moral postulates, including their ethical implications, are even more important than in other countries of the EU, since the ethical norms are supported with their legally enforceable equivalents.

Technology is increasingly being globalized as are the ethical implications of its applications. However, one cannot neglect the differing – and, behind the converging legal regulation, still decisive – traditions, values, societal systems of countries of the cultural East, which are at the forefront of developing and applying new technologies. In such cultures the characteristics and borderlines of human dignity may be different, individual freedom and self-determination may have a different role (not entirely absent, as certain Western stereotypes state, but have a different role and significance), as well as their legal guarantees, if there are any; and the distinction between the living and the lifeless, animate and inanimate may be less important than in the cultural West. The latter, for example, may be manifested in a different judgment on human-machine symbiosis, or more tolerant attitudes towards the “numbering” of people, or towards robots, especially those that are anthropomorphic or animal-like.

We hypothesize that in the foreseeable future in the area of the specific ethical implications of emerging technologies only some universal principles and their legal representations may be expected at the global level. However, it seems reasonable to assume that European norms and expectations will continue to be of “higher” standards than in some other parts of the world, as we consider those to be higher if they reflect the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights. Therefore it is not only the ethical nature of developing and applying emerging technologies that should be promoted within a European value system, but Europe’s impact on other regions of the world would also gain significance in this area.

If we accept that decision-making in the EU, including decisions regarding emerging technologies, is permeated by community law, and one of the fundamental tasks of community law is to represent values, including moral values, we must also agree that the ethical aspects must always be included in these decisions, implicitly or explicitly. Consequently, from a legal point of view, questioning whether ethical considerations are adequately observed equals questioning lawfulness. Therefore, in the analysis we do not need to start from scratch, nor to envision a completely new ethical and legal system, or to define completely new principles, but we need to build upon the existing legal system of the EU and the system of law and values of the Member States constituting its grounds.

Taking the general pace of legal development into consideration, within the time horizon of our research, which is 10–15 years, a dramatic transformation of legal systems, especially under the conservative umbrella of the EU, cannot be expected. However, the relationship between legal and technological development is not the only area where different paces can be observed: more significant is the pace of social changes which cannot be expected, nor required to be controlled by technological development (although the influence of technology is evident), and even more important is the pace of changes in societal values, which superficially seems to be fast but these values can be regarded as rather stable at the deeper levels.

### **3. Technology-related lawmaking and its enforceability**

A further basic reason why it is not necessary to introduce totally new principles and legal branches is the rigidity and inertia of technology-regulating (or rather technology-following) legal instruments. Until lawmakers really grasp the essential characteristics and modes of application of a given specific new technology, understand their whole range of impact on legal and societal relationships, and until the draft laws or regulations pass the various levels of lawmaking, the specific technology or application often becomes obsolete or has already resulted in circumstances which cannot be retroactively modified or even remedied. That is why legal regulation should define principles, functions and requirements, drawn from the experience (or anticipation) of using specific technologies, rather than provisions regulating the specific technologies themselves.

An important principle in technology-related lawmaking is the technology-neutrality of the law. According to this principle, first introduced in the Electronic Communications Privacy Act of the USA (1986), later widely adopted in EU regulation, as analyzed by Koops (2006, pp. 83-90), the same general rules should apply to legal relationships involving the use of new/emerging technologies in question as to those involving other technologies, or no technologies at all. Although both the meaning and the function of this principle can be debated – as Reed (2007) argues, technology neutrality is not as natural and desirable in ICT regulation “as motherhood and apple pie” (pp. 264-266) –, its application can prevent both the suppression of the developing and use of any technology and the unfair favoring of one technology over another. It also prevents those not using any technology from being put at disadvantage compared to those using technologies. However, one should take into account that new technologies may create circumstances on the individual, group and societal levels alike, which have not existed before. Similarly, certain circumstances may arise directly from the application of a given technology.

There are furthermore definitional problems in technology-related lawmaking. At a general level, the legal notions are indirectly influenced by the metaphors used to describe abstract phenomena or entities. According to popular perception the computer is a machine, while in the foreseeable future the notion of “computer” may lose this meaning (see, for example, ambient intelligence) or may become something representing certain functionalities of the human brain. It might be possible to comprehend the essence of technologies and their implications in a holistic way but it might still be impossible to define the technology or the

implication itself. The law, however, basically employs exact definitions, and it may be difficult to give precise, not too narrow and not too broad definitions for an emerging technology and all its future implications. Nevertheless, if lawmakers form proper definitions, judges and other involved actors can be capable of applying the norms adequately.

There are relatively few legal professionals educated in the new, information-related or technology-related legal areas, who are able to understand the legal and ethical implications of new and emerging technologies. It is essential that such professionals be employed not only as advisers or lawyers serving the interests of the business selling technology-based services, but also in public administration and judicature.

In addition, there is a well-known but often latent reluctance, even resistance, to any legal or ethical norm limiting the possibilities of scientific and technological development among those working in the R&D area as well as those introducing new technologies at the business or political levels. If those interested in developing and applying emerging technologies regard legal and ethical norms as unreasonable border conditions of their work, one may not expect law-abiding or ethical behavior on their part. That is why voluntary self-regulation has an increasing potential in this area.

Finally, monitoring and supervision of the enforcement of legal provisions relating to the development and application of emerging technologies are rather difficult. Therefore control mechanisms should be fast and efficient in this area, with appropriate intervention points, otherwise legal regulation may easily become obsolete and lose trust of society in general and those involved in developing and using emerging technologies in particular.

#### **4. Legal and ethical implications of specific emerging technologies**

Following our approach, according to which the law is supposed to reflect, and be able to enforce, moral requirements, we examined the need and the possible ways of transforming such requirements into binding legal norms in the area of specific emerging technologies. We explored in particular the legal and ethical implications of the use of affective computing, ambient intelligence, artificial intelligence, virtual and augmented reality, bioelectronics, neuroelectronics, cloud computing, future internet, human-machine symbiosis, and robotics.

It can be observed that certain groups of emerging technologies require smaller, other groups require greater changes in the existing legal system. Smaller changes are necessary where such technologies are, at least partly, covered by existing general legal norms and standards. For example, in the area of applying emerging technologies, which have privacy and data protection implications, the existing fundamental principles and technology-neutral provisions can be applied. The use of other technologies may require technology-specific legal responses, such as exceptions to the general rules, or higher standards of protection of individuals. In addition, certain emerging technologies may require profound changes in several branches of law, for instance, in the areas of criminal liability, non-contractual liability, as well as public administration procedures such as the accreditation of new devices.

After having examined the above range of specific emerging technologies, we came to the conclusion that similar ethical concerns, and, consequently, similar or analogous legal issues, emerged in certain groups of technologies. We are aware of the fact that the conceptual borderlines of emerging technologies are sometimes blurred – not to speak about their foreseeable convergence – and their classifications can be criticized from several aspects. For the purpose of this study, we found that the following three groups of technologies raised common questions, due to the similarities in their functions, setting and operation: (1) *network-based technologies* (including ambient intelligence, cloud computing, future internet), (2) *interface (“cyborg”) technologies* (human-machine symbiosis, neuroelectronics, bioelectronics, virtual/augmented reality), and (3) *artificial intelligence based technologies* (artificial intelligence, cognitive systems, advanced robotics, affective computing).

1) In the area of *network-based technologies* the extending of already existing and elaborated legal frameworks such as the general rules and principles of data protection – see a comprehensive overview by Bygrave (2008) – may be necessary. Since these technologies are based on the combination and integration of information and communication technologies, it is absolutely non-essential for the user what technology he or she is actually using, or interacting with, and the privacy implications of using such network-based technologies are obvious. The possibility of introducing ambient intelligence or creating a global network of physical objects (“smart things”) unavoidably leads to applications going far beyond the purpose they have been developed originally (e.g. monitoring health status, ordering milk by the fridge itself, or making impaired or disabled people’s life easier). This is why lawmakers should declare the principle of purpose-limitation (originally elaborated in the area of data protection) concerning emerging technologies at a general level, prescribing that a given technology must be applied only to the extent necessary to achieve the legitimate purpose(s) specified by the law. By doing so, lawmakers should define the scope and purpose of the use of such technologies and avoid a situation where the end justifies the means – i.e. the technology justifies the purpose.

International and national law should work out in detail the legal provisions applicable to the complex situations network-based systems may create. Regarding cloud computing this should include the conflicts arising from the territorial nature of national laws, as well as labor law provisions regarding the “virtual companies” operating in a complex legal and IT environment. Although data protection lawmaking is technology-neutral and thus may be adapted to emerging technologies, legislators should take into consideration that individuals’ rights might not be appropriately protected by current data protection regulation against potential infringements caused by network-based technology applications. Consequently, lawmakers should review data protection issues in order to examine their applicability to network-based systems, and, where needed, they should adjust the regulation to the challenges of these technologies by creating additional regulatory instruments. To give an example, in a cloud computing environment certain requirements of legitimate data processing such as the “freely” given and the “informed” character of the consent to data processing activities (European Union, 1995) as well as the concept of individuals’ informational self-determination, originally developed by the German Federal Constitutional Court (1983), become doubtful if no additional guarantees are created.

From the legal point of view, the location of service providers – more precisely, data controllers – plays a significant role in handling cloud computing risks in the EU. It is a key characteristic of cloud computing that computers being used for processing and storing consumers' data can be located at any point in the world, thus service providers can easily escape from the scope both of EU law and Member States' competence. Even if they stay within the scope of EU, in a cloud computing environment data circulate freely among EU Member States via the Internet, therefore it is no longer clear which data protection authority is responsible for ensuring the supervision of implementation of data protection requirements (Widmer, 2009). Lawmakers must find solutions to these problems. The use of "data havens" (territories outside of the jurisdictions providing higher level protection of rights or prescribing certain duties) should be restricted by legal means.

Specific legal provisions are necessary to guarantee the transparency of data controlling and processing activities in cloud computing environments, see Gartner (2010). This is the only way for data subjects to retain some chance of keeping their personal data under control, and for authorities to be capable of following the implementation of privacy rights. Lawmakers should take into account here that business logic and business interests do not explicitly stimulate cloud service providers to be as transparent as they are supposed to be. Users of cloud computing services may have the impression that they are using a desktop application, however, in reality, their data are processed in a distributed environment where transparency and control are guaranteed at a fundamentally different – lower – level. Service providers must be obliged by law to make their consumers aware of this difference.

To work out the detailed legal relationships – especially the division of responsibility – between the data subject, the data controller (service provider) and the third party (who has access to the distributed data) is also a necessary task of the lawmakers. In addition, distributed services at the IT level may mask strong centralization at the organizational, administrative or political levels. All legal provisions which provide guarantees for the division of informational power or restrictions on the centralization of the controlling of personal data should be extended to the situations arising in cloud computing environments.

2) In contrast to network-based technologies, in the area of *artificial intelligence based technologies* lawmakers can probably no longer rely solely on existing fundamental principles. The melding of the organic and the non-organic, the living and the lifeless, the virtual and the real may result in such life situations that the law has never faced. Therefore artificial intelligence based technologies will undoubtedly call for making – at least some, but rather a number of – alterations in several branches of law.

On the basis of the aforementioned, there should be legal guarantees for human users of systems based on artificial intelligence to make them aware of whether they are confronted with another human (e.g. an officer or a call center employee) or with an intelligent system. Thus the human user would be able to exercise her rights in such situations, with special regard to the restriction of automated decision-making, which already forms part of EU and national laws.

The law should define those generic characteristics of advanced humanoid or animal-like robots the presence of which would prohibit users to treat such robots in ways already prohibited in the case of treating humans, such as torture, bestiality or humiliation (see e.g. Lin et al., 2009, pp. 53, 61). Such a prohibition should be independent of whether the robots themselves are regarded as entities in possession of rights. Manufacturers and service providers should be responsible for preparing and regularly updating ethical codes regarding the developing and use of robotic systems. Military and law enforcement agencies should be responsible for guaranteeing that no simulation programs using virtual reality may present military or law enforcement actions as games or otherwise losing the feeling of responsibility for killing people or infringing their basic human rights. Such a responsibility should be extended to both training and the representation of the activities of such agencies in the media.

Manufacturers and service providers should also be obliged by law to build an emergency shutdown system into advanced robots which can limit the basic functionality of these devices. The emergency shutdown system should be activated automatically in case of certain behaviors or situations which may get out of control regarding the original functionality of the robots, or in case if the robot's activity may endanger humans or the environment directly, or lead to unlawful circumstances. Such a system should also allow external activation.

Legal regulation should also prescribe the compulsory form and content of information to be made available about the extent of possibilities and consequences of using, or entering into interaction with, robots. The law should prescribe the compulsory and uninterrupted use of a standard visual (audiovisual) marker in virtual environments where the sensory appearance or behavior of the elements of the virtual/augmented reality (objects, humans, living creatures) become similar to those of such elements in the real world. Such systems, applications, as well as individual uses of such applications should also offer the continuous possibility to leave the virtual environment without delay.

3) *Interface technologies*, especially neuroelectronics, bioelectronics and human-machine symbiosis show the difficulty and complexity of the tasks of the law, which has to regulate interdisciplinary fields including computer science, cognitive science, neurosurgery and biomedical engineering. These technologies may result in dangerous effects on the human body and human nature as well as on society itself. Considering that certain possible applications of interface technologies can go far beyond the original purpose of developing such technologies, and this might lead to serious violations of fundamental rights, it is essential to specify the legitimate purpose(s) of such applications.

By defining the appropriate standards for manufacturing and using neuro- or bioelectronic devices, lawmakers have to bear in mind, among other things, that the use of such devices may seriously violate the requirement of equality. Human and human must not significantly differ from each other. Neuroelectronic technologies offer possibilities to change the abilities of humans (Allhoff et al., 2010), and this may not serve solely the purpose of making disabled people's life easier but also providing unnatural and disproportional advantages to



their possessors (eyes seeing in an extended spectrum of light, enhanced smelling, artificial abilities to reason and remember, etc.) Considering that the implanted neuro- or bioelectronic devices function inside the body in an invisible way, it is difficult to keep their use under control, especially because the use of such devices (biosensor, biochip, or artificial organ) should also be considered as a privacy matter. Law should reflect upon this conflict through balancing the interests involved.

Although we understand law as general rules that apply equally to everybody, the exceptional circumstances of a person wearing a biosensor or biochip may require exceptional regulations, too. (For instance, at present the pain or discomfort caused by seatbelt-pacemaker contact is noted as an exception from the general obligation to fasten the seatbelt in cars in a number of countries.) Other questions to be answered by law include the rules of division of responsibility among the user, her physician and the manufacturer.

Law must also protect the personal integrity of people wearing neuroelectronic devices. It should be emphasized that personal integrity is not only a question of data protection, but also a question of human dignity. Dignity expresses the human dimension of life and thus is an elevated and absolute respected value. In order to protect individuals from harmful interventions, law must ensure the integrity of neuroelectronic devices. Biochips must not be susceptible to any "attacks" and in special cases must be protected from the individuals themselves as well. The realization of such principles requires standardization in this area, too.

Furthermore, intelligent interfaces, which are embedded in everyday objects and are aware of one's preferences and needs, may seriously compromise individual autonomy. The logic of anticipatory personalization may result a manipulative world where possibilities for making "respective decisions" become questionable.

## **5. Speculative findings**

If we review the foreseeable consequences of the large scale application of specific emerging technologies or technology groups, and analyze them together with the consequences of the spreading of the present new technologies (which were emerging technologies a few years ago), we can identify cross-cutting trends that require reactions from the part of legal regulation, the role of which is to transmit ethical norms.

In the following we present our findings in two categories: first, from the aspects of the appliers and users of emerging technologies, and second, from the aspects of the lawmakers expected to regulate the use of such technologies.

***A. From the aspects of those applying and using emerging technologies:****Technologies become less transparent.*

It can already be seen in the case of new technologies widely used today, and can be foreseen even more in the case of emerging technologies, that the operation of applications and services based on such technologies becomes less and less transparent, both for those applying such technologies and for the end-users of the services. Maintaining this opacity may be in the interest of the service providers who do not want to make their services transparent in order to enforce their interests in lawful or unlawful ways. Adequate legal regulation, together with its enforcement (monitoring and sanctioning tools), may have an important role in counterbalancing this trend.

*Responsibilities may be blurred.*

In complex transactions involving many players, including individuals, organizations and non-human participants in possession of highly developed intelligence, determining responsibility, and if needed, enforcing thereof, may lead to a blurred legal situation. This could be counterbalanced by clarifying and refining legal regulation regarding the division of responsibility among the manufacturer, the user and other involved actors.

*Auditing becomes more difficult.*

As the borders of administrative and business entities become more ductile, the permeability of these borders increase, and the borders of the underlying information infrastructure becomes blurred, defining the criteria of operating of such entities (both from the IT and the business aspects) becomes difficult. Therefore the logging of operation of such entities, as well as detecting and auditing their operation differing from the expected, may also be difficult. Working out adequate rules is primarily the task of professional organizations but law should define its framework.

*There is less chance for voluntary participation.*

In a free society and constitutional democracy the self-determination of individuals may only be limited by similar rights of others or by rules absolutely necessary for the operation of the State. Already in the environment of today's new technologies, but even more in that of the emerging technologies, the chances of those living in modern societies for enforcing self-determination (in practice: voluntariness and informed consent) are eroding fast. Therefore it is of utmost importance for lawmakers to work out the criteria and legal guarantees of ensuring personal autonomy in the environment of new and emerging technologies.

*New type inequalities may arise.*

Besides the already known inequality in connection with new technologies (haves and have-nots) other type inequalities may also increase, such as the inequality caused by restricted access to new technologies for political considerations, by restricted access to new technologies for religious or ideological reasons, or the generational inequality arising from the pace of technological development. Even the well-known effect of machines superseding human workforce (but also creating new working possibilities) may have new dimensions:

the spread of robots serving elderly or ill people may have an effect on immigration since such functions are traditionally fulfilled by immigrants in some societies. Law should, on the one hand, support unrestricted access to technologies and services, on the other hand, facilitate reducing of inequalities by offering possibilities for affirmative actions.

## **B. From the aspects of lawmakers:**

*The time of intervention by legal regulation has special importance.*

Considering the ever increasing pace of technological development, and the irreversible nature of certain essential economic, political and social impacts, legal regulation – where necessary – should come into existence in a phase when it is able to substantially influence the developing and spread of applications and services based on emerging technologies, or in certain cases even the directions of developing the technologies themselves.

*Self-regulation may have an important role.*

The chances of enforcing law or the voluntary following of legal provisions will significantly decrease if legal regulation will not be accompanied, on the one hand, by stimulating changes in the system of interests (that is an economic and political issue but it should be reflected in law, too), on the other hand, by working out ethical norms for researchers, developers and applicers of emerging technologies (that is an issue of self-regulation). The preparation of means of self-regulation, for example, ethical codes or codes of conduct, and the most important elements of such codes may be made obligatory by law but the working out of such codes should expediently be made by the professional or representative bodies of the respective areas.

*Multilevel governance provides an opportunity for EU-level harmonization.*

The multilevel structure of governance of the EU raises the question: on which level the individual implications of emerging technologies shall be handled with respect both to the principle of subsidiarity and the question of efficacy. When weighing up this question one should take into consideration that the fundamental principles guiding the European Union (the rule of law, respect for human rights, equality etc.) must be reflected at national levels of governance as well, however, the European regulation must respond to the demands of the aforementioned cultural and societal diversity of Member States. Since the multilevel system is functioning as a cross-border network, it provides the opportunity for Member States to exchange their experiences regarding emerging technologies.

*Communication between lawmakers and other stakeholders is a regular task.*

Regular communication is necessary between the lawmakers and the other stakeholders (researchers, developers, service providers, users), partly in order to share information arising in rapidly changing environments, partly in order to jointly clarify legal and ethical principles in the area concerned, even in cases when direct interests would expectedly hinder consensus.

*Definitions and legal authority should be clarified.*

Lawmakers should work out an adequate and coherent system of notions and definitions regarding the use of emerging technologies and should also provide for its regular review. Similarly, when defining the scope of legal documents a balance should be found between the application of the principle of technology neutrality and the need for specific regulation of distinctive life circumstances created by emerging technologies.

## **6. Empirical findings**

If researchers of the legal and ethical implications of emerging technologies aspire to formulate guidelines for the legal profession in general and the lawmakers in particular, first they need to explore the existing situation in the area of legal regulation. We therefore conducted an empirical research in order to establish whether EU level legal regulation reflects the challenges posed by emerging technologies at all. We deem this survey empirical in the sense of studying the reality of EU legal regulation.

In the course of the empirical study we used legal databases covering the whole corpus of EU law (directives, decisions, international agreements and other acts). In order to perform the survey we used the search engine available through Westlaw International, since this database covers the whole corpus of EU materials, and its query functions are of high quality. The scope of the present research did not permit us to scrutinize the entirety of legal sources of the EU, even less to analyze in detail the legislation and regulation of Member States of the EU with respect to the ethical implications of emerging technologies.

The findings are, on the one hand, of quantitative nature: they present *the number of occurrences* of terms relevant to the subject in the whole legal corpus of the EU; on the other hand, the findings are of qualitative nature: according to the occurrences of terms in the hierarchy of legal sources and their relevance, we drew conclusions regarding *the manifest representation of emerging technologies and their ethical implications in EU law*.

At first we selected 50 keywords or terms relevant to the emerging technologies examined by the ETICA project – the framework of our study (<http://www.etica-project.eu>) –, 2-7 terms per technology. We investigated the occurrences of these terms in the legal corpus of the EU. Certain terms, which are otherwise well-known both in professional and popular literature, such as bioelectronics, nanorobot, software robot, interactive computing etc. cannot be found anywhere in the whole of the EU legal databases. Most of the remaining terms occurred in only a few documents, and only a few terms seemed to be popular and widely used in the EU legal corpus, such as ambient intelligence (in 23 documents), artificial intelligence (39), future internet (22), internet of things (29), and virtual reality (31).

However, even the high number of occurrences of search terms (altogether 182) may be misleading. On the one hand, certain terms can be used in different meanings, e.g. “autonomous agent” can also be used in a general, metaphoric sense, as was the case in an advocate’s opinion concerning the Case C-303/06 of the European Court, saying that “[w]hen we act as *autonomous agents* making decisions about the way we want our life to

develop our personal integrity and sense of dignity and self-respect are made concrete"; or in an opinion of the European Economic and Social Committee, "the initial response should come from the social partners, *as autonomous agents*." In other cases the terms occurred only in references to other materials.

On the other hand, many of the documents containing a relevant keyword relating to emerging technologies are various versions of the same documents: drafts, opinions, proposal for a decision, amended proposal for a decision, the decision itself etc. Furthermore, the fact that exactly the same sentences can be found in different documents relating to the search term concerned illuminates the way these documents have been created: at times only by copying from existing sources. The majority of the remaining, "clean" hits are only preparatory acts (staff working documents, draft documents, communications, proposals for Commission decision, opinions) passed by various EU institutions. The two binding legal acts (two regulations) among the hits do not contain rules concerning emerging technologies. Directives have not been passed in this field at all.

The substantial documents deal with the theme of emerging technologies only at a very general level. A typical example from a report of the Commission: "It is hoped that this research will lead to the development of a new generation of biosensors and biochips and these will be used, for instance, in health and environmental monitoring, food analysis and/or toxicology studies." (Joint Research Centre, 2003, p. 17) A rare example of concrete provisions can be found in a European Parliament recommendation (European Parliament, 2009, p. 8) concerning fundamental rights aspects of the internet of things. According to this recommendation, the Council is suggested to draw attention to the fact that the development of the "Internet of things" and the use of Radio Frequency Identification (RFID) systems should not sidestep the protection of data and of citizens' rights".

Although an empirical study of this level is not suitable for drawing conclusions in a statistical sense, it can be observed that *the relevant terminology of emerging technologies is not represented in the EU legal documents*. We amended our research with some general search terms, such as emerging technologies (134 hits), new technologies (2671), or new ICT (260). Naturally the scope of the present study did not allow us to open every document in this category, only randomly selected ones. It could however be established that most of the documents use the enlisted general terms at a very general level.

We can conclude that the legal implications of emerging technologies are not reflected in the EU legal documents and attracted only a minimal legislative attention in the competent bodies of the EU. Neither regulations, nor directives have been passed in this area. Legislation relating to emerging technologies basically remains in the sphere of supporting specific research programmes. The aim of such programmes however is to support the developing of new technologies and this does not include the examining of social and legal impacts. Although these supported research and development projects in the area of emerging technologies may serve as inputs for the constructing of legal frameworks, the intent of constructing such legal frameworks, or the need thereof, cannot be discovered in these projects.

The only technology the legal implications of which have been noticeably taken into consideration by EU institutions is Future Internet (Internet of Things). The establishing of the "Expert Group of the Internet of Things" on 10 August 2010 should be regarded as a progressive step within the overall passivity of the EU in this area. The group's task is to advise the Commission on how best to address the technical, legal and organizational challenges of Internet of Things at European level.

## 7. Conclusions

As can be seen from the foregoing analysis, applications of emerging technologies raise a number of profound ethical and legal issues that are inseparable from each other. It can also be observed, on the basis of the empirical findings, that the EU level legal documents hardly reflect the challenges posed by emerging technologies.

The legal norms, which transmit the general values of human dignity, freedom, democracy, equality, the rule of law and respect for human rights, and which should be taken into consideration when developing and using emerging technologies, are formulated at a rather abstract level, therefore they may have only a minor impact on researchers, developers, service providers and users. Considering that the law has an intermediary role between the abstract ethical norms and the reality, it has the mission of reflecting on the moral challenges and ethical implications of emerging technologies. By doing so, the law can handle the obvious conflict between the high generality of moral principles and the thorough details of their application in the environment of practical use of emerging technologies. However, there are several steps to be taken in the process of accomplishing this mission.

First and foremost, a new set of basic principles and criteria should be worked out in detail for the use of emerging technologies, with special emphasis on individual choice, consent and transparency. Existing principles from international documents such as the data protection principles should be adapted and adjusted to the new circumstances. The principle of purpose specificity should be extended to emerging technologies. Although technology is not neutral in itself (similar ICT support can be used, for example, for laying and for removing of land mines), still the choice must not be regarded as a mere question of freedom of scientific research.

Taking Privacy Impact Assessment as an example, the principles and methodology of Ethical Impact Assessment should be worked out. (In the area of information technology, see Wright, 2010.) Before any substantial technological change which might lead to ethical controversies, such an assessment should be performed.

Considering the complexity of legal implications of emerging technologies, such technologies may constitute a separate area of law in the not-so-distant future. For that reason, up-to-date information and practice regarding emerging technologies should not be left out from education in law. Legal science should work out adequate regulatory strategies for different scenarios regarding the developing and applying of emerging technologies, including the convergence of separate technologies.

Adequate forums should be established in order to ensure regular communication between lawmakers and other stakeholders (researchers, developers, service providers, users) in the areas of emerging technologies. An adequate and coherent system of notions and definitions regarding the use of emerging technologies should be worked out and regularly reviewed.

Lawmakers should create a legal environment inspiring self-regulatory acts based on commonly accepted principles.

Finally: norms are not legal norms by nature only because they are embedded in provisions of a legal document issued by the legislative powers of the sovereign. Any norm, even with the strongest moral or ethical background, becomes a legal norm with legal nature if its enforcement is guaranteed. Consequently, the key success factor of handling ethical implications of emerging technologies by legal solutions is the establishing of fast and efficient control mechanisms, which are responsible for the enforcement of laws regulating the use of such technologies any time in the future.

## References

Allan, T.R.S. (2003), *Constitutional Justice: The Liberal Theory of the Rule of Law*, Oxford University Press, New York, NY.

Allhoff, F., Lin, P., Moor, J. and Weckert, J. (2010), "Ethics of Human Enhancement: 25 Questions and Answers", *Studies in Ethics, Law, and Technology*, Vol. 4 No. 1, Article 4, available at [http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1003&context=phil\\_fac](http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1003&context=phil_fac) (accessed 6 March 2011)

Bygrave, L.A. (2008), "International Agreements to Protect Personal Data", in Rule, J.B. and Greenleaf, G. (Eds.), *Global Privacy Protection: The First Generation*, Edward Elgar Publishing Ltd., Cheltenham, UK, pp. 15-49.

Dyzenhaus, D., Moreau Reibetanz, S. and Ripstein, A. (Eds.) (2007), *Law and Morality: Readings in Legal Philosophy*, University of Toronto Press, Toronto.

Dworkin, R. (1996), *Freedoms' Law: The Moral Reading of the American Constitution*. Harvard University Press, Cambridge, Mass.

European Parliament (2009), "European Parliament Recommendation of 26 March 2009 to the Council on Strengthening Security and Fundamental Freedoms on the Internet", available at <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0194+0+DOC+XML+V0//EN> (accessed 6 March 2011)

European Union (1995), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, *Official Journal of the European Communities*, L 281, 23/11/1995, pp. 0031-0050.

European Union (2000), "Charter of Fundamental Rights of the European Union (2000/C364)", *Official Journal of the European Communities*, 18.12.2000, pp. 364/1-364/22.

Gartner (2010), "Gartner Global IT Council for Cloud Services Outlines Rights and Responsibilities for Cloud Computing Services", available at <http://www.gartner.com/it/page.jsp?id=1398913> (accessed 6 March 2011)

German Federal Constitutional Court (1983), "Volkszählungsurteil", BVerfGE 65, 1

Howard, M.M. (2003), "Postcommunist Civil Society in Comparative Perspective: An Empirical Baseline", in Howard, M.M., *The Weakness of Civil Society in Post-Communist Europe*, Cambridge University Press, Cambridge, UK.

Inglehart, R. and Klingemann, H-D. (2003), "Genes, Culture, Democracy, and Happiness", in Diener, E. and Suh, E.M. (Eds.), *Culture and Subjective Well-Being*, MIT Press, Cambridge, MA, pp. 165-183.

Joint Research Centre (2000), "JRC Annual Report 2000", European Commission, COM/2001/0239 final/

Klingemann, H-D., Fuchs, D. and Zielonka, J. (2006), *Democracy and Political Culture in Eastern Europe*, Routledge, Abingdon, UK.

Koops, B-J. (2006), "Should ICT Regulation be Technology-Neutral?", in Koops, B-J., Lips, M., Prins, C. and Schellekens, M. (Eds.), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, TMC Asser Press, The Hague, pp. 77-108.

Lin, P., Bekey, G.A. and Abney, K. (2009), "Robots in War: Issues of Risk and Ethics", in Capurro, R. and Nagenborg, M. (Eds.), *Ethics and Robotics*, AKA Verlag, Heidelberg, pp. 49-67, available at: <http://works.bepress.com/palin/3> (accessed 6 March 2011)

Reed, Ch. (2007), "Taking Sides on Technology Neutrality", *SCRIPT-ed*, Vol. 4 No. 1, pp. 263-284, available at <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.asp> (accessed 6 March 2011)

Tamanaha, B.Z. (2004), *On the Rule of Law. History, Politics, Theory*, Cambridge University Press, Cambridge, UK.

Smith, J. C. (1968), "The Unique Nature of the Concepts of Western Law", *The Canadian Bar Review*, Vol. 46 No. 2, pp. 191-225.



Székely, I. (2007), "Central and Eastern Europe: Starting from Scratch", in Florini, A. (Ed.), *The Right to Know. Transparency for an Open World*, Columbia University Press, New York, NY.

Székely, I. (2010), "Changing attitudes in a changing society? Information privacy in Hungary 1989–2006", in Zureik, E., Harling Stalker, L., Smith, E., Lyon, D. and Chan, Y.E. (Eds.), *Surveillance, Privacy and the Globalization of Personal Information. International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, London, Ithaca, pp. 150-170.

United States of America (1986), Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22, available at [http://www.law.cornell.edu/uscode/18/usc\\_sup\\_01\\_18\\_10\\_I\\_20\\_119.html](http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_119.html) (accessed 6 March 2011)

Widmer, U. (2009), "Cloud Computing and Data Protection", available at <http://www.whoswholegal.com/news/features/article/18246/cloud-computing-data-protection/>

Wolchik, S.L. and Curry, J.L. (2008), *Central and East European Politics: From Communism to Democracy*, Rowman & Littlefield, Lanham, MD.

Wright, D. (2010), "A Framework for the Ethical Impact Assessment of Information Technology", *Ethics and Information Technology*, Springer Science+Business Media B.V., Online First, 7 July 2010, available at <http://www.springerlink.com/content/a6g05r6331224448/fulltext.pdf> (accessed 5 March 2011)

Zureik, E., Harling Stalker, L., Smith, E., Lyon, D. and Chan, Y.E. (Eds.) (2010), *Surveillance, Privacy and the Globalization of Personal Information. International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, London, Ithaca.