

## **EDITOR'S NOTE**

Wim Muller<sup>\*</sup>

The contributions in this issue of the European Journal of Legal Studies tackle various developments which are currently shaping our future and raise important questions, varying from what technological advances mean for our understanding of “law”, to how legal tools are devised in practice to deal with the challenges posed by new advances. The topic is introduced below by the members of the Infosoc Working Group of the Department of Law of the European University Institute, who organised the conference during which these contributions were first presented and were kind enough to honour the European Journal of Legal Studies by publishing them in this Special Conference Issue. On behalf of the Editorial Board of the Journal, I would like to thank the members of the working group for all the work, and Benjamin Farrand for further editorial assistance. We are pleased to offer our readers a this collection of thought-provoking essays.

---

<sup>\*</sup> Editor-in-Chief, European Journal of Legal Studies.

## **INTRODUCTION: LOOKING INTO THE FUTURE...**

Meritxell Fernández-Barrera, Primavera De Filippi, Norberto Nuno  
Gomes de Andrade and Mario Viola de Azevedo Cunha<sup>\*\*</sup>

In the future humankind will find itself in an incredibly automatic and intelligent new space, people will be surrounded by technologies that observe, monitor, analyse, interpret, simplify, anticipate and explain the world for us. Humanity will be immersed in a deep and permanent communicational status, living in a planet of machines, agents and automatic processes. A vast array of powerful interfaces, embedded in all kind of objects and gifted with some sort of intelligence, will capture, scrutinise and process data about reality and nature surrounding us, as well as about every other human being living within. Such agents will recognise, react and respond, in an intuitive manner, to the presence and to the actions of different people and electronic objects. Human action and decision-making will be increasingly delegated to artificial agents, reality visible to the human eye will be super-imposed by electronic tags, digital identifiers and virtual entities, and the current network of computers and other terminals called the Internet will be a network of digital people, sharing a half-fictitious, half-real space that visionaries have been for long time prophesising as cyberspace or metaverse and that is now becoming to reality under the denomination of ubiquitous computing and ambient intelligence.

The future will be dominated by interactive technologies, pervasive and ubiquitous computing, mixed realities (where the virtual and the physical realms will converge), ambient technologies, augmented reality, autonomous software agents, artificial intelligence and many other technological developments.

### **“THE FUTURE OF ...” - CONFERENCE ON LAW & TECHNOLOGY**

Taking a glimpse beyond the present and bearing in mind the possible and prospective technologies which will come to fruition in the future, the European University Institute (EUI), through the Law Department and in conjunction with the InfoSoc Working Group, organised "The future of... Conference on Law & Technology," hosting the event in Florence, on 28 and 29 October 2008.

The conference challenged the academic community to think and foresee

---

<sup>\*\*</sup> *InfoSoc* Working Group, European University Institute, Florence, Italy

what challenges, problems and changes the Future will bring to Law. Rather than preview what the future will look like, the conference aimed at collecting new ideas, concepts and theories of how Law will accompany such a future, proposing a creative exercise in which a description of the upcoming world was combined with a prospective analysis of how law will change and evolve.

The conference intended to provide an original and ground-breaking symposium for exchanging ideas and fostering the debate about the triangular relationship between future, law, and technology, attracting quality papers dealing with prospective studies and analyses of legal developments and transformations expected in the future. Taking into account the present technological trends affecting society, the “Future of...” Conference challenged scholars to think about and foresee the main problems and changes that Law will face and suffer in the upcoming future of ambient technologies, ubiquitous and pervasive computing, web 3.0, entangled realities, autonomous software agents, artificial intelligence and many other features and elements.

The conference welcomed the contributions of scholars and researchers from many different regions and cultures in the world, whose interests and research were directed towards the assessment of the evolving relationship that might develop in the future between law and technology. The numerous contributions were clustered into six different panels:

- General issues. New dimensions in the technological environment:
  - the role of the law and agency
  - Public law, jurisdiction, boundaries
  - ICT tools for the law
  - The personal sphere in the technological milieu: Liberty and privacy
  - Biotech
  - Intellectual property. Copyright, patent law

#### **SESSION I: GENERAL ISSUES. NEW DIMENSIONS IN THE TECHNOLOGICAL ENVIRONMENT: THE ROLE OF THE LAW AND AGENCY**

The first session of the Conference, entitled “General issues – New Dimensions in the technological environment: the role of law”, presented two papers which analysed the interaction between law and technology, each one focusing on different aspects of this intricate relationship. The first paper, authored by Massimo Durante from the University of Turin, argued in favour of a role of mediation between the real and the virtual world assigned to law within the future evolution of information and

communication technologies (ICT). The second paper, written by Sawhney, Ratnadeep and Lee, highlighted the importance of metaphors and precedents as conceptual tools to understand the development of new technologies.

Durante, through his paper “Re-designing the Role of Law in the Information Society: Mediating between the Real and the Virtual”, argues that, notwithstanding the incessant technological evolution, law will keep having an autonomous and central epistemological role in representing reality. In this account, law will be assigned the essential role of mediation between the real and the virtual world. In the words of the author, such an act of mediation requires a translation of the virtual information displayed by technology (the possibility opened and made available by the application of new ICT) into real information.

In developing his main argument, Massimo Durante claims that law, assigned with the role of mediation between the virtual and the real, will ensure the conditions of reliance upon information in both directions: from the virtual reality to the real world and from the real world towards the virtual reality. Regarding the former, law is attributed with the epistemic role of appraising in what terms the effects of an action performed in the virtual reality can be judged foreseeable and thus accountable in the real world (such effects are to be appraised in terms of legal responsibility, as it is within the real world that one is responsible for [the effects of] actions displayed within virtual reality). In addition, law displays its role of mediation also in the opposite direction, i.e., from the real world to the virtual reality. In this case, law confers a real content to the real world that can be appraised within virtual reality (this is done by means of informational reliance, as it is within virtual reality that one relies on informational data in order to perform actions that are likely to produce [legal effects] within the real world). In this perspective, and as Durante asserts, law can play a fundamental role of mediation between the real and the virtual to the extent that it assures reliance upon information. Moreover, as the author concludes, the way in which law can devise an act of mediation which determines the conditions of possibility of the representation of what is refereed to as “virtual reality” within the realm of what is referred to as “physical reality” and vice versa is structured by the inter-subjective computer-mediated interaction and communication between individuals or groups.

The second paper, entitled “New Technologies and the Law: Precedents via Metaphors” and co-authored by Harmeet Sawhney, Venkata Ratnadeep Suri and Hyangsun Lee (Department of Telecommunications, Indiana University, Bloomington), provides an interesting study on the

application of metaphors by courts as conceptual tools to understand and regulate new technologies. In legal terms, and as metaphors help to establish precedents, the paper explains how new communications technologies have been shaped by legal precedents created by previous ones.

The article, relying upon a historical study of US case law, demonstrates how metaphors, in some cases, can be effective vehicles for the transfer of conceptual frameworks from one technology to another (as in all point-to-point networks that transport materials and information from one point to another – electric grids, highway systems, telegraph, railroad and telecommunications networks); and how, in other cases, this metaphor process breaks down (as in the case of radio and broadcasting, in which its initial conception as “wireless telegraph” or a point-to-point communication technology caused intricate juridical problems). The authors use the example of radio as a case where a metaphor based on an old technology failed to shape the new one in its image, describing the phenomenon of a “metaphor vacuum”, i.e., a case in which there were no readily available metaphors to think about the new broadcasting technology. Departing from the problem of “metaphor vacuum”, within the example of broadcasting as a new technology for which no clear precedent had been established, the article investigates how the legal system dealt with such a “stalemate”. Since the case law could not proceed without a precedent, the authors observe how such tension was resolved by “stretching” a previously established metaphor. Such a stretching process is carried out until it reaches a breaking point, which creates a metaphor vacuum or a realisation that a radically new framework is needed. Broadcasting technology is used by the authors as a paradigmatic case, as it ended up with a standard from the world of transportation systems and public utilities through the insertion of a new standard of “public interest, convenience and necessity” (PICON). In other words, PICON filled the metaphor vacuum, bringing along with it a legal framework.

This article calls our attention to the fact that, in the future, metaphors used in the early stages of the development of a new technology may not prove to be appropriate in the long run, setting precedents difficult to change at a later stage. It is thus important to remember that the “devil is in the details”, i.e., to remain alert to the peculiarities of the new technology, as it is the peculiarities that eventually bring about a metaphor vacuum.

## **SESSION II: PUBLIC LAW, JURISDICTION, BOUNDARIES**

In the second session of the Conference, entitled “Public law, jurisdiction,

boundaries”, the three papers presented deal with the need to regulate the internet, but each one with a different aim. In the first paper, Armando Cottim analyses the interaction between cybercrime (and cyberterrorism) and the boundaries of criminal law jurisdiction. As the author states, “the advent of cyberspace has changed the established criminal law model. Online crime happens without boundaries, as attacks can come from outside the borders of one State, thus scattering crime scenes through two or more countries, sometimes in more than one continent.”

With this in mind, he analyses the 2001 Budapest Convention on Cybercrime, starting with an overview of all possible jurisdiction theories to be applied, and concludes that the “Convention relies exclusively on the territoriality and nationality theories to empower parties to establish jurisdiction.” Cottim criticises the choice made in the Convention, believing that it creates more problems than solutions.

Then he discusses the threats that arise from the interaction between Cybercrime and Jurisdiction, where he presents the famous *Yahoo Case*, decided by *Tribunal de Grande Instance de Paris*, “which ordered Yahoo! Inc and its subsidiary Yahoo France not only to exclude French surfers from sales of Nazi memorabilia (...), but also to destroy all the concerned files stored in their server”, and goes also through the *Rome Labs* and *Tore Tvedt* cases.

After discussing these cases, and the issues that can arise from the impact of cybercrime and cyberterrorism on the jurisdiction of the States, Cottim concludes that “cyberterrorism would probably not justify a convention to deal with it. The explicit inclusion of cyberterrorism in the Convention on Cybercrime by means of an additional protocol would probably suffice”. However, “given the path towards catastrophism and indiscriminate attack on human lives taken by modern day terrorism,” he “would consider possible and positive the inclusion of terrorism in the list of international crimes against humanity – in accordance with littera k of number 1 of article 7 of the Rome Statute of the International Criminal Court (ICC) – which would entitle States to have universal jurisdiction to apprehend terrorist agents, although jurisdiction to prosecute would be given to the International Criminal Court.”

The second paper “Children Protection Online: Uneasy Steps towards a Balance between Risks and Freedoms”, presented by Federica Casarosa, focuses on the European initiatives for the protection of Children concerning the use of internet, what is a very important issue, since “children and young people are more and more often the first to take up and use new technologies; yet, they are not always aware of both risks and

ways of dealing with them, or, whether they are, they are not always mature enough to evaluate the situations that they encounter and the possible consequences their decisions can have.”

The author recognises that sometimes the content to which children and young people have access through the internet is legal, at least for an adult, but it is “liable to harm them by impairing their physical and mental development” (COM(96) 87, par. 17).

After analysing the European framework in this area, she describes all existing risks for children in accessing the web: child abuse material; child grooming; cyber-bullying; and, unlawful privacy invasion. Then, Casarosa presents the tools developed by the European Union to fight against these risks (Hotline networks, Rating and filtering schemes, Age verification tools and Codes of Conduct).

Finally, she analyses the case of “social networks” (such as Facebook or Myspace) to conclude that “any policy aimed at protecting children, either from illegal and harmful content or from other possible online risk, due to the nature of the subject-matter, should be of a multi-faceted nature.”

The last paper, by Oles Andriychuk, entitled “Concept of “Network Neutrality” in the EU Dimension: Should Europe Trust in Antitrust?” aims at giving “a descriptive presentation of the current European regulatory framework in the areas of electronic communications and audiovisual policy”.

In his paper Andriychuk analyses the evolution of the EU legislation in the field of telecommunications, highlighting that the European policy in this area “was supposed to be governed by three major principles: liberalisation, harmonisation and competition”. Then, having these principles as a starting point, Andriychuk addresses the contradictions that arise from them, saying that “[t]he main problem is based in their ontology and methodology.”

He discusses issues concerning the “European policy of limited profitability” and “Local Loop Unbundling”, and, then, moves his focus to the European law of electronic communications, which he calls “Present-day regulatory regime”. In this topic he draws a comparative analysis between the EU and the US concerning “Network Neutrality”, stating that in the EU this issue “has been neither settled, nor yet properly articulated”. Although, he believes that since public opinion plays an important role in the European decision-making process, “the perspectives of the ‘Network Neutrality’ legislation appear to be quite likely”.

Andriychuk concludes that “Network Neutrality’ is an interdisciplinary phenomenon. It can be explored from economic, legal, societal, technical and political dimensions.

As we could observe, all the papers, in one way or another, deal with the interaction between the Internet and law addressing how law can provide an up to date response to this new phenomenon, trying to find a solution which guarantees the protection of the individuals without blocking the development of such technology.

### **SESSION III: ICT TOOLS FOR THE LAW**

Session III, entitled “ICT tools for the law”, was conceived as a section to explore the characteristics and implications of the use of ICT support for legal practice. It was thus concerned with the area of study known as “Legal Informatics”, “Artificial Intelligence and Law” or “Information Technology for lawyers”, among other possible expressions.<sup>1</sup> Whereas IT Law deals mainly with the issue of analysing which are the legal problems of the new reality arising from the use of Information Technologies and how to tackle them, legal informatics is technologically oriented and explores how computer applications can be best developed to meet legal practitioners’ needs. This implies a contextualised understanding of technological applications and requires, therefore, a thorough analysis of current trends and needs in the legal profession. This is precisely the main focus of Prof. Pompeu Casanovas’ paper entitled “The Future of Law: Relational Justice and Next Generation of Web Services”, in which he intends to bridge the evolution of web technologies (Web 2.0, Web 3.0, next generation Semantic Web) with the change of paradigm in the legal field. Prof. Casanovas carries out a detailed study of current technological trends (Web 2.0, Web 3.0, Semantic Web) and prospects of application in the legal milieu. He underlines the fact that there is a current lack of knowledge of the detailed way in which the Internet is evolving, and that some of the Semantic Web promises have not yet been fulfilled. New trends such as the next generation of web services based on personalisation and user-centred approaches are discussed. The incredible expansion of the legal market as well as the pervasive use of ICT in legal practice are presented as indicators of what is going on in the legal sphere. Some current trends in the intersection between law and technology are highlighted, such as the obstacle that the law sometimes represents for

---

<sup>1</sup> A. OSKAMP and A. LODDER, “Law, Information Technology and Artificial Intelligence”, in A. LODDER and A. OSKAMP (Eds.), *Advanced Technology in the Legal Domain. From Challenges to Daily Routine*, Dordrecht, Springer, 2006, p. 3.

technological evolution, and the effect the use of new technologies has in the expansion of the legal profession. In this framework a new legal paradigm is introduced, through the concepts of Relational Law and Relational Justice, based on flexibility, dialogue and autonomy, on a higher and more effective citizen participation and the increase of self-regulatory forms, all of which can be enhanced by the next generation of web services. This creates a general picture of the future of the law, underlined by the main thesis of the paper: that Semantic Web technologies should be cognitively and sociologically grounded in order to satisfy real user needs, taking thus into account “the social situated knowledge that enables law to be created, implemented and shared in an increasingly technological social and organisational environment.”

The concept of legal informatics has indeed evolved following technological advances and requirements from the users in the legal profession. It started with the construction of the first databases of legal documents in the 1960s, giving way later on to the design of large administrative databases in the 1970s, to systems aimed at assisting lawyers in the task of finding legal information (legal information retrieval) and to great expectations in the field of expert systems in the 1980s, which would turn out later on to be too ambitious a programme. Nowadays approaches to legal informatics have changed perspective and regard computer applications as assistance tools to the main task accomplished by a human operator. This assistance can focus on the different information processing tasks that are part of the legal professional daily routine, one of which is legal information retrieval. This has always been central to legal reasoning, but especially nowadays, when risk of information overload exists, enabling more efficient access to reliable and useful legal knowledge becomes a pressing need. Indeed, legal information of different types (authoritative sources but also case law and legal doctrine<sup>2</sup>) is moving to the Web and therefore legal professionals, and citizens as well, are exposed to information overload.

Geist’s paper, entitled “The Open Revolution: Using Citation Analysis to Improve Legal Text Retrieval” focuses precisely on the improvement of legal information retrieval systems, which are still based on the same technologies that were used in the 1980s (mainly Boolean search) even if the system performance presents deficiencies. The paper proposes an improvement by the introduction of citation analysis, which is an information science concept according to which citation can indicate the

---

<sup>2</sup> G. SARTOR, M. BIASIOTTI, E. FRANCESCONI, M. PALMIRANI, F. VITALI, *Legal Informatics and Management of Legislative Documents*, Florence, European University Institute, 2007.

existence of a relationship between documents. Citation analysis was used to improve the performance of the Google search engine and the author of the paper highlights the feasibility of applying it to the search of information in the legal domain, since the network structure of the www and that of legal documents is similar. Indeed, the case study of the paper shows that the network structure of Austrian Supreme Court decisions and their headnotes is a free-scale one, just like the www network structure.

Sometimes legal informatics not only provides new tools for the assistance of traditional legal tasks, like legal information retrieval or legal drafting, but proposes the introduction of new tasks or methods for legal analysis at the same time that it provides tools to support these newly suggested tasks. This is the case in the article by Mahler on “Tool-supported Legal Risk Management: A Roadmap”. The first part of the paper presents the advantages of the introduction of a method for legal risk analysis. This implies an innovation in legal method, for even if risk management exists *de facto* in legal practice, no formal methodology has been developed by legal theory in this regard. The paper provides a definition of legal risk and illustrates through an example how a standardised method for dealing with legal risk could be applied to the assessment of the clauses of a contract. Nevertheless given that methods for legal risk assessment are still not well established, the author argues, they should be regarded as a complement to current legal methods, which are based on experience and heuristics. Furthermore, since the introduction of legal risk management methods is complex and costly, the introduction of IT support could be very valuable. The second part of the paper suggests three ways in which IT tools could support the task of assessing legal risk: by supporting the process, helping the analyst to follow an order and to document the outcomes at every stage; by supporting the communication between different experts, which might be required to identify the risk and estimate it; by ensuring interoperability with existing legal information systems. The author claims as well that, with due care, it would be possible to include some elements of automation to support human judgment and analysis in legal risk assessment. Finally some considerations are made with regard to the limitations that legal risk analysis might have as a business model, due to its costs, but further research is encouraged in light of the potential benefits it might bring about.

Beyond their application to the support of legal activity, IT, and especially Artificial Intelligence, can be regarded as possible risk sources for some rights. Calo’s paper explores precisely this aspect of AI, by analysing its current developments and potential dangers for the right to privacy and how US privacy law can cope with those challenges. The approach taken in

this paper is therefore different from the one taken in the previous ones: in this case, technology is analysed as a factor that alters reality and can, therefore, require a reaction from the law in order to prevent certain undesirable effects. The paper starts with an overview of the traditional concern about dangers of AI for privacy. Traditionally, AI threats to privacy have been connected to the increased capabilities of AI enhanced devices not only for surveillance, but for the organisation and the analysis of data in such a way that new information may emerge which was not previously obvious to the human eye (data mining and knowledge discovery). The paper goes on to analyse the current trend of enhancing the social capabilities of machines, in order to make them interact more naturally with people. It highlights as well some of the effects of social machines on people, among which the elicitation of human-directed behaviour and the increase of the sense of being observed and the corresponding feeling of uneasiness. These are controversial issues with regard to the right to privacy. Firstly, given the reaction of people to social cues present in the behaviour of machines, the collection of information by the latter will become easier, since they are endowed with an ability to persuade subtly. Secondly, the pervasiveness of social AI may hinder the possibility of being left alone in private spaces in which to be oneself with the corresponding limitations for the development of one's personality. Finally, as to the way in which US privacy law deals with the highlighted risks for the right to privacy, the author claims that the law contains already some answers, although education and other extra-legal solutions (like discussions around social media) are feasible as well, especially in the short term.

#### **SESSION IV: THE PERSONAL SPHERE IN THE TECHNOLOGICAL MILIEU: LIBERTY AND PRIVACY**

In the fourth session of the Conference, "The personal sphere in the technological milieu: Liberty and privacy", all papers addressed the new challenges to privacy as a consequence of the recent development of information technologies, focusing, however, on different issues. The first paper, entitled "Property in Personal Data: a European Perspective on Instrumentalist Theory of Propertisation", analyses Lessig's theory of privacy as a property right from a European perspective. Such a model of data protection, which leaves to the individual the possibility to decide whether personal information can be used or not, goes in an opposite direction of the European model, which considers the right to personal data as an autonomous fundamental right, which confirms the importance of such a right for the European society.

To develop this analysis, Purtova raises the question of "whether the

introduction of the property rights in personal data, whatever scope of those rights may be, is a legal option in the European Union”.

After considering that the introduction of property rights in personal data would be “a legal option in the EU, both on the level of the Union and individual member states”, she concludes “that content-wise Lessig’s instrumentalist theory does not fit into the European legal context because the scope of rights in personal data it advocates for is not what is meant by property in Europe.”

Different from Purtova, in the second paper - “The Myth of Odin’s Eye: Privacy vs. Knowledge” - Paolo Guarda discusses the risks of the access to knowledge in a digital context for individuals’ privacy. He believes that individuals are not aware of the cost of our access to knowledge in a digital context, “despite the outward gratuitousness of the provided service”.

He analyses the cases of Digital Rights Management systems (DRM) and of “Google search engines”, addressing the issues that arise from the relationship between privacy and knowledge in the digital context.

Guarda identifies “three fundamental dimensions of the concept of privacy: ‘spatial’, ‘informational’, and ‘decisional’”, linked to the consumption of intellectual works, and focuses his analysis on the last dimension, which he defines as the one that “concerns the choice, the freedom that must be recognised to every person in order to be able to take a decision without any kind of external conditioning.”

Finally, after analysing many aspects of what he calls “privacy vs. knowledge conflict”, Guarda suggests that we should reconsider “rules, technologies, and customs in the light of this new unifying category that moves our attention to the management aspect of the exchanging flows, rather than to their inherent diversity.”

From the descriptions above, we can see that both authors tried to draw our attention to the challenges that new technologies pose to Law and the need to find solutions that balance all interests involved and are in line with the current digital scenario.

## **SESSION V: BIOTECH**

Session V of the Conference was devoted to biotechnology and to the potentialities that this scientific field promises to set off. Biotech is dramatically changing the world we live in, questioning our own human constitution and nature, and challenging many of our legal assumptions,

principles and theories. Biotechnology is, at the present time, one of the most exciting areas for interdisciplinary research, presenting a panoply of troublesome questions and problems in the fields of agriculture, food science and medicine, among others.

One of the most interesting developments in the area of biotechnology relates to genetic engineering technology and its application to the human body, allowing for the genetic manipulation of the latter. Regarding this theme, Wojciech Zaluski's paper analyses the question of the admissibility of enhancing an embryo's nature through genetic engineering (calling this process genetic enhancement), tackling this question from a legal philosophical point of view, through an argument of autonomy.

The paper provides a number of important and necessary distinctions and articulations that one should bear in mind when examining the question of genetic enhancement and autonomy, such as personal and moral autonomy (and its different varieties: material and formal, weak and strong); their corresponding presuppositions; and the different types of genetic enhancement, the directed genetic enhancement and the all-purpose genetic enhancement. While arguing that personal autonomy does not have any presuppositions, Zaluski does not take a definite position concerning moral autonomy, asserting that it is not clear whether the latter has two (human agency, free will) or three presuppositions (being contingency of birth the third one).

In this account, the author distinguishes two competing conceptions of moral autonomy, one that does not presuppose contingency of birth (conception I) and the other that presupposes (conception II). Regarding such problematic presupposition, Zaluski questions Habermas' claim that contingency of birth is crucial for moral autonomy, being a presupposition of human agency. According to the German philosopher, a person whose birth was not contingent cannot be expected to be able to take full responsibility for her actions, and thereby cannot be morally autonomous. Zaluski, contrarily, does not find it self-evident that human agency requires that a subject's genetic constitution should not have been designed by some other person, asserting that the lack of contingency of birth does not by itself undermine human agency. In this regard, Zaluski presents arguments supporting the claim that contingency of birth is not (necessarily) a presupposition of human agency and thereby of moral autonomy. Nevertheless, the author leaves the question open, safeguarding the position of those that advocate contingency of birth as presupposition of human agency.

Finally, the fundamental question posed in the paper, the question of

genetic enhancement and the violation of human autonomy, receives different answers according to the articulation established between the two conceptions of moral autonomy and the two types of genetic enhancement.

## **SESSION VI: INTELLECTUAL PROPERTY. COPYRIGHT, PATENT LAW**

Session VI of the Conference was concerned with the future of intellectual property in the digital environment, with particular focus on the forthcoming developments of copyright law in the information society. As it is becoming an increasingly valuable asset, in fact, information has been progressively turned into a commodity, whose value can however only be exploited if appositely supported by legal and/or technological means.

In particular, the advent of digital technologies has considerably affected the production and distribution of works in the realm of intellectual property. Their impact can mostly be attributed to the increasing digitalisation of content and to the growing trend towards globalisation that is characteristic of the Internet network. These new technologies have made it possible for nearly anyone to produce and/or reproduce a whole variety of works and to disseminate them via the Internet, regardless of any legal or national boundaries.

Enforcing copyright law in the digital environment has therefore become a challenge that may jeopardise the traditional business models employed by the entertainment industry. While a new set of offences has become available on the Internet, the scale and the extent of the more traditional offences have in fact been considerably amplified. Digital technologies also have destabilised the two fundamental features of the copyright regime: the concept of artificial scarcity - originally meant to realign the properties of intangible works with that of physical goods - and the notion of exclusivity, implemented through a set of exclusive rights which are strictly and inherently national. This raises the following questions: Is the current IP regime still appropriate in the digital environment? Is it still necessary in order to protect the incentives to create and to disseminate new content? And most importantly, is it sensible to protect an intangible work in the same way as we protect a tangible one?

From authors to end-users, from producers to commercial publishers, copyright law has a different impact on every party involved. While the digital environment may be regarded as a threat by certain categories of people, for others, the Internet and digital technologies constitute an exceptional tool for the production and dissemination of content.

It is commonly believed that stronger laws against the unauthorised reproduction and distribution of content (such as the DMCA in the US and the Directive on the Information Society in the EU) are necessary to provide effective remedies against copyright infringement. Yet copyright enforcement will never be successful as long as users do not consider the provisions of the copyright regime to be fair. Therefore, the need for public legitimacy should not be underestimated. If overly restrictive, copyright law will be either infringed upon or in some way circumvented, whereas an excessively lenient regime will inevitably be ignored.

Originally conceived for the purpose of encouraging cultural production, copyright law has been designed to provide authors with sufficient economic rewards through the granting of proprietary rights in the expression of any original work of authorship. It has nevertheless always been acknowledged that the protection granted by the copyright regime had to be somewhat limited, both in scope and in duration, since an optimal level of innovation could only be achieved with the establishment of a proper balance between private property and public domain.

This particular issue is explored by Federico Morando in his paper on “The legal status of software interoperability information” in which he addresses the uncertainty regarding the legal status of interoperability information by distinguishing between interface specification and interface implementation. The paper provides a thorough analysis of the actual scope and limitations of copyright protection for computer software and related interoperability information, and concludes by suggesting that certain categories of works, such as most utilitarian works, should be subject to a weaker form of protection designed to discourage free-riding without hindering the process of cumulative innovation.

Thus far, the flexibility of copyright law has allowed for the copyright regime to readjust to and/or to overcome a multitude of historically challenging circumstances, as evidenced by the increasing number of works that copyright protection has been granted to. Today, however, new solutions are being devised by the private sector, which is seeking autonomously to address the challenges introduced by the digital environment, albeit from two opposite perspectives. On the one hand, insofar as it can be assimilated to a private good, information has been made excludable and artificially scarce by means of restrictive contractual agreements and technological measures of protection. On the other hand, to the extent that information is being regarded as a public good, widespread availability can be achieved through specific contractual mechanisms, such as Open Content licences, which may encourage the widespread dissemination of works while ensuring that right holders retain

a certain number of their rights.

Yet the effectiveness of private ordering depends on a variety of legal and technological factors. As highlighted by Ugo Pagallo in his paper on “The future of P2P systems and their impact on contemporary legal networks”, there exists a mutual interaction between technological progress and legislative activity. On the one hand, the development of new technologies necessarily requires traditional legal concepts to be readjusted or reformed. On the other hand, however, the legal system will determine the direction into which a particular technology may or may not develop. Accordingly, as technological advances necessarily have an impact on the legislation, the law is equally capable of affecting technological progress by either endorsing or condemning specific technological developments. Technology is, therefore, not neutral and public regulation may sometimes be required to either promote or constrain certain private mechanisms of self-help in order to allow for the deployment of new contractual and/or technological innovations.

With the introduction of an additional layer of protection for any technological means replicating the physical properties of private goods, legislative reforms have been so far endorsing private regulation only to the extent that it was intended to restore the former status quo.

However, like most areas characterised by risks and uncertainty, the digital environment may actually represent a tremendous opportunity for a variety of stakeholders. For instance, the entertainment industry once regarded the VCR as a threat, although a valuable business model has eventually grown out of this threat: the rental industry. The Internet, if appropriately exploited and regulated, would definitely yield similar benefits.

Indeed, since stronger IP laws may actually hamper the potential for the creation and dissemination of works, Internet and digital technologies should perhaps be embraced as an opportunity for innovation rather than being addressed as a dangerous threat.

The law nonetheless has an important role to play as far as the endorsement of a certain technology is concerned. As Ugo Pagallo demonstrates in his paper, with the advent of P2P technology, we may eventually witness the deployment of a more efficient way of producing and distributing information through the Internet. However, while the law may attempt to control its development, it is only by allowing the technology to develop independently that its corresponding benefits and drawbacks will become objectively identifiable and capable of being

consequently dealt with. Instead, banning or excessively regulating a new technology at the outset would merely stifle technological progress and eventually prevent the emergence of new and more efficient business solutions.

The set of papers presented at the conference shows the richness of the debate that arises from the complex question of the future panorama of the entanglement of law and new technologies. On the one hand, the development of technologies gives place to new realities not previously foreseen by the law at the time of its creation. In this sense it is very illustrative to think of Simon's concept of an artefact and to apply it analogously to the law. An artefact is designed according to its functionality, taking into account the environment in which it is expected to work:

“An artifact can be thought of as a meeting point –an ‘interface’ in today’s terms– between an ‘inner’ environment, the substance and organization of the artifact itself, and an ‘outer’ environment, the surroundings in which it operates. If the inner environment is appropriate to the outer environment, or vice versa, the artifact will serve its intended purpose. Thus, if the clock is immune to buffeting, it will serve as a ship’s chronometer. (And conversely, if it isn’t, we may salvage it by mounting it on the mantel at home.)”<sup>3</sup>

If we understand the law as an artefact, designed taking into account a particular reality that it intends to regulate (outer environment), it will be natural to think of the necessity of adapting it if that reality changes. In our case, due to new technological advances and specially to their pervasiveness, reality changes and many issues arise that need a legal answer. The topics of the panels of the conference are just an example of the issues requiring further legal attention: from the right to privacy and liberty, to intellectual property debates, and issues of public law, like the boundaries of jurisdiction in the digital milieu, cybercrime and the regulation of biotechnology, among others. On the other hand, however, technologies can bring about many benefits that cannot be ignored and that have indeed received attention during the conference. In particular ICT and AI can provide increased functionalities for computer support to the tasks that are part of legal practice, such as legal information retrieval or legal drafting. This is a sign that due to scientific and technological development not only the object of legal analysis evolves, but legal practice itself changes as well in its methods and cognitive underpinnings.

---

<sup>3</sup> H. A. SIMON, *The Sciences of the Artificial*, Cambridge, MA, MIT Press, 1969, p. 9.

This way, even if predicting the future is not an easy task, we strongly believe the conference to at least have provided a forum of discussion for exploring open issues and current trends, in which a fruitful exchange of ideas and impressions to deal with future events in the field has taken place.

**RE-DESIGNING THE ROLE OF LAW  
IN THE INFORMATION SOCIETY:  
MEDIATING BETWEEN THE REAL AND THE VIRTUAL**

Massimo Durante

**I. THE AUTONOMY OF LAW: AN EPISTEMOLOGICAL PERSPECTIVE**

The aim of my paper is to envisage how the role of law will be re-designed in relation to the evolution of information and communication technologies (ICT). The hypothesis proposed in this paper is that law will keep having an autonomous and central *epistemological* role in representing reality, namely, in providing a mediation which will enable us to bridge the physical and the virtual realms, the empirical convergence of which does not account by itself for the construction of a common epistemological ground.

This hypothesis is not intended to underestimate the change determined by the technological computer-based revolution, which tends to transform “the basic nature or the scope of the activity or institution”<sup>1</sup> to which technology applies. The transformation of reality resulting from technological developments is not only quantitative but also qualitative: the computer-based technological revolution not only widens the range of our own interrogations but it also changes the meaning of our questioning.<sup>2</sup> In more appropriate terms, this means that, even though transformation (which applies both to the world and to human beings)<sup>3</sup> is a crucial key in order to understand the technological evolution, a qualitative analysis does not research, in the transformed phenomenon (object, activity, institution or human being), the explication of the transformation (the technical principle). Such explication is to be researched in the transformation of the inquiry through which this phenomenon is investigated and cognitively represented.

When reflecting upon a determined activity realised by means of a technological device, we first ask ourselves how efficiently the computer performs this activity. Once the technological application has become part

---

<sup>1</sup> J. MOOR, “What is computer ethics?”, in T. WARD BYNUM (ed.), *Computers & Ethics*, Malden Mass., Blackwell Publisher, 1985, pp. 266-275.

<sup>2</sup> In this perspective see M. DURANTE, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, Torino, Giappichelli Editore, 2007, pp. 28-29.

<sup>3</sup> N. WIENER, *Cybernetics: or Control and Communication in the Animal and the Machine*, Cambridge (Mass.), MIT Press, 1948, and *The Human Use of Human Beings*, Anchor, Doubleday, 1954.

of the performance of such an activity, then we ask ourselves what are the nature and the value of this activity. This stratified inquiry governs how a phenomenon transformed by the technological evolution is progressively investigated and cognitively represented as being part of the technological reality. The evolution of technology not only plays a role in determining reality but also in shaping its representation and appraisal.

This is the reason why, when we reflect upon the consequences of the application of technology to the world of law, we end up wondering about the nature of law and the direction of its evolution of law, which is not only empirically but also conceptually absorbed within the ongoing technological revolution. This direction is necessarily connected with the direction of the technological revolution, which is mainly expressed by the ability to rapidly<sup>4</sup> transform the world and determine, from an epistemological perspective, a specific reality made of both an analogical and a digital dimension. This line of evolution is focused upon a representation of the world as subject to continuous transformation: the world (which is the referent of the discourse about globalisation, *mondialisation*<sup>5</sup>) is considered more and more in its own possibility, in its virtual or possible states-of-the-world, rather than in its positive reality, namely, in its fixed or stable dimension. In more philosophical terms, it is the case of a (representation of the) world in which what is held as *stable* (what we can rely upon either to take a decision or to behave) is no longer determined nor explained by an ontology founded upon the positive existence of a material, real object, but by a different and new ontology, founded upon the non-contradictory content of an information that is concerned with the possible states-of-the-world. This ontology cannot be simply accounted for in terms of a digital ontology as opposed to an analogical ontology. Both of them are only epistemological descriptions of the world<sup>6</sup>, which cannot pretend to state what reality is (metaphysics) but only how reality can be experienced and conceptualised by an epistemic agent at a given level of abstraction (epistemology). In this line of research, it appears more promising, for instance, to envisage an *informational ontology*, according to which knowledge of the world is knowledge of its structures (intended as sets of data)<sup>7</sup>.

<sup>4</sup> See on this point P. VIRILIO, *La vitesse de libération*, Paris, Galilée, 1995, and *Vitesse et politique*, Paris, Galilée, 1977. On this perspective see S. REDHEAD, *Paul Virilio: Theorist For An Accelerated Culture*, Toronto, University Press of Toronto, 2004.

<sup>5</sup> J.-L. NANCY, *La création du monde ou la mondialisation*, Paris, Galilée, 2002.

<sup>6</sup> A. LESNE, "The Discrete versus Continuous Controversy in Physics", in *Mathematical Structures in Computer Sciences*, 17 (02), pp. 185-223.

<sup>7</sup> L. FLORIDI, "Against Digital Ontology", in <http://www.thephilosophyofinformation>.

## II. LAW AS LEGAL SCIENCE: STABILIZATION OF EXPECTATIONS AND MEDIATION

Intended as legal science, law has always played a paramount role in the epistemological perspective, namely, in the representation of reality. Legal science has constructed the possibility to mediate between the real (*what is*) and the virtual (*what ought to be*) reality within the physical domain. The virtual reality of law (*what ought to be*) has never been only an infinite adjournment of the real world (*what is*) but it has always entailed a specific form of reality with its own language, consistency and categories (legal science). In addition to this, we should notice that law has not only served as a mediation between the virtual and the real world but it has also set the limits of representation of one term within the epistemological domain of the other, through the distinction between *de facto* (the phenomenon to be represented in legal terms) and *de iure* (the conditions of possibility of representation) questions.

However, this distinction belongs more to the epistemology of law than to a description of reality, that is to say that such a distinction accounts for a different and layered representation of how reality can be understood rather than for a description of how reality is: this does not mean that law produces its own reality (*constructivism*) but only the means to represent and understand it, precisely in the topological sense in which a map (that is both a mean and a piece of knowledge) represents a determined space, in order to reduce the complexity of such environment and allow people to orientate themselves within it (*ecological information*).

The evolution of law that stems from the technological computer-based revolution has, thus, to be considered primarily from a theoretical point of view, namely, from an epistemological perspective, rather than from a merely empirical one. As pointed out, we should never lose sight of the fact that law is not only concerned with the control of critical situations but is *epistematical* in itself, *i.e.* capable of producing a specific knowledge. Within the framework of the information society, where information is meant to entail an ordered series of possible states-of-the-world and therefore regularity, the evolution of law has to be thought of as the evolution of the science of what is *possible*, intended in a Kantian sense, as what possesses a *non-contradictory content* and it *conforms to the conditions of both intuition (de facto) and thought (de iure)*<sup>8</sup>.

---

<sup>8</sup> See on this point, G. DICKER, *Kant's Theory of Knowledge. An Analytical Introduction*, Oxford/New York, Oxford University Press, 2004, p. 79: "For Kant, to say that something is possible is not to say only that it is logically possible or free of

Contradiction has always nourished law, which has also been conceived as the attempt to overcome contradiction. The possible contradiction between the functioning of the virtual and of the real world, *i.e.* the consistency of the digital and analogical reality, is likely to undermine or at least to menace the conditions of possibility of an ordered communication within the society of information. The question is not to oppose a disposition to change (technology) to a pretension to stability (law). On the contrary, it deals with the recognition of what can be taken for *stable* in what changes, in order to make the flow of information and communication ordered and effective. In other words, law is likely to be kept charged with the role of stabilisation of expectations, but we should wonder what it means now to stabilise expectations within the networked information society.

The role to be assigned to law cannot be limited in the networked society of information to the norm's predictive power, on the basis of which the norm is expected to foresee and measure human behaviours and to govern reality. How can law govern reality, when the latter is subject to continuous transformation? Law is not to be opposed to the technological evolution (both law and technology belong to, and thus stem from, the development of human culture) but is meant to progressively become part of the informational system. In our view, law will be (kept) charged with an essential role, namely, the role of *mediation* between the real and the virtual world.

### III. THE CONCEPT AND ROLE OF MEDIATION

Mediation is the action of serving as intermediary between two terms: *i.e.* one term, from which the reasoning starts, and another term, to which the reasoning is leading, since the act of mediation is the condition for the representation of the second term within the epistemological realm of the first one.

The concept of mediation is based on a philosophical assumption, which is central to our analysis, namely that nothing is simply given as a stable, assured basis for something else. In epistemological terms, nothing is either immediately present in its conceptual meaning or is evident by itself in the thought process (neither the "real world" nor the "virtual reality").

---

contradiction: this is a necessary condition but not a sufficient one. Rather, to say that something is possible means that it conforms to the conditions of both intuition and thought; as Kant states it in the First Postulate: 'That which agrees with the formal conditions of experience, that is, with the conditions of intuition and of concepts, is *possible*'".

This was already affirmed as the fundamental principle of Kantian epistemology: intuitions without concepts are blind, concepts without intuitions are void.<sup>9</sup> On the contrary, every phenomenon is to be represented and thought of by means of mediations. In this perspective, mediation is not conceived as a simple relation between two terms, since a relation compounds two already established terms. Mediation is intended as a dynamic process of thought (such as a legal reasoning) within which progressive connections represent and establish terms. Through the act of mediation, something (phenomena, terms or data) can be assumed as the stable basis for the representation and the comprehension of something else.

The concept of mediation denies abstract unrelatedness, and affirms the possibility of complex relatedness among phenomena. Therefore, mediation entails, from an epistemological perspective, a denial of a world (both real and virtual) of unrelated elements. On the contrary, it endows the world with the possibility of communication between the real and the virtual. A mediated world turns out to be more than the sum of static, empirical relations among agents of the real and the virtual world: it grows out of the communication process between epistemological stances and exists in the tension of their mutual becoming a *real* and a *virtual* world. In this perspective, the act of mediation is the condition of representation of the virtual reality within the epistemology of the real world and vice versa. This allows one term or entity of the real/virtual reality to be taken as the stable basis for the representation and comprehension of another term within the epistemology that describes how the real/virtual world can be experienced and conceptualised by an epistemic agent at a given level of abstraction.

For instance, while punishing the online theft of identity, made possible by the current informatics' technologies, we do not only judge a behaviour as being illegal, but we also endow the *virtual* identity with a *real* consistency, by delimiting to what conditions it is possible to rely upon the set of data concerning the online personal identity. In this perspective, as outlined

---

<sup>9</sup> A significant interpretation of Kantian epistemology is offered by J. MCDOWELL, *Mind and World*, Harvard, Harvard University Press, 1996, p. 3: "The overall I am going to consider in these lectures is the way concepts mediate the relation between minds and the world. I shall focus the discussion in terms of a familiar philosophical outlook, which Donald Davidson has described as a dualism of scheme and content. That will get us quickly to Kant. One of my main aims is to suggest that Kant should still have a central place in our discussion of the way thought bears on reality". And p. 4: "So the picture is this: the fact that thoughts are not empty, the fact that thoughts have representational content, emerges out of an interplay of concepts and intuitions".

before, we end up qualifying, at least to some extent, *what is an online personal identity*, not only in strict, legal terms, but rather at the level of inter-subjective communication, *i.e.* of symmetrical and mutual reliance on information.

As a term can be represented and assumed as the stable basis for something else, this provides the epistemic agent with a predictive power. Such a predictive power shall be judged according to the interplay of the real and the virtual world within the information society. Since there is no prediction without representation, the conditions of possibility of representation set the structural limits of any predictive power. These conditions of possibility are to be considered within the epistemology of law, which assumes such conditions as the necessary presuppositions of the norm's predictive power.

The prediction set forth by the norm of positive law displays an informational content that enables us to stabilise our expectations. It allows us to behave in a free manner, namely, by foreseeing and measuring the predicted effects of our actions. This informational content appears to be, however, more and more static compared to the transformation of the world (this is an old argument renewed by the technological evolution) and to the flow of informational resources shared throughout the networks (this is a new argument determined by the information and communication technologies). The informational content of the norm is likely to rapidly become contradictory with the augmented reality of the infosphere, *i.e.* "the whole informational environment constituted by all informational entities (thus including informational agents as well), their properties, interactions process and mutual relations".<sup>10</sup>

In this perspective, law has to become part of the informational system; in contrast to a widespread opinion, this does not mean that law is either overcome or determined by technology. On the contrary, law keeps its own specificity, precisely thanks to its ability to mediate between the real and the virtual world. This act of mediation requires a translation of the *virtual* information displayed by technology, namely, the possibility opened and made available by the application of new ICT, into *real* information. The reality of information is no longer based upon the positive existence of a real, material object; actually, it is based upon the *non-contradictory* content of information, on which it is held reasonable to rely, in order to take a decision and behave.

---

<sup>10</sup> L. FLORIDI, "A look into the future impact of ICT on our lives", <http://www.philosophyofinformation.net>, p. 3.

From this consideration a basic principle should be inferred and established as a firm premise of our line of reasoning: it is possible to set an ordered form of communication only on the basis of reliance upon relevant information,<sup>11</sup> shared at an inter-subjective level.<sup>12</sup> The inner rationality of the multi-agent system of the networked society of information is not to be found in a set of certainties (from which the legal order ought to be deduced) but in its attitude to cope both with the flood of information deriving from the upgrading of social networks and the structural *lack of knowledge*<sup>13</sup> characterizing the asymmetry between environmental and systemic information.

#### IV. MEDIATING BETWEEN THE REAL AND THE VIRTUAL IN THE INFORMATION SOCIETY

According to our opinion, in the information society law will be thus mainly meant to play the role of mediation between the virtual and the real, namely, to ensure the conditions of reliance upon information in both directions: a) *from the virtual reality to the real world*: in this context, the concept of virtuality is endowed with a real content constituted by the idea of foreseeable consequences, whose importance and extension are progressively subject to the convergence of online and offline life. This delineates, according to many authors, the most relevant trend of the networked information society: “Nowadays, we are used to considering the space of information as something we log-in to and log-out from. Our view of the world (our metaphysics) is still modern or Newtonian: it is made of ‘dead’ cars, buildings, furniture, clothes, which are non-interactive,

---

<sup>11</sup> See T. MALDONADO, *Reale e virtuale*, Milano, Feltrinelli, 2007, p. 151: “Nessuno può ormai negare che la nostra percezione è satura di valori e disvalori, di giudizi e pregiudizi; sostenere però che essa non ci dica nulla di credibile sulla realtà mi sembra una conclusione abusiva. E il punto riguarda direttamente la questione del rapporto virtuale-reale. Perché, in ultima istanza, tutta la controversia sulla realtà del virtuale e sulla virtualità del reale è inseparabile dal problema dell’affidabilità (o meno) della nostra percezione del mondo reale”. See also T. BERNERS-LEE, *Weaving the Web. The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*, New York, Harper One, 1999.

<sup>12</sup> In this perspective see M. DURANTE, “What Model of Trust for Networked Cooperation? Online Social Trust in the Production of Common Goods (Knowledge Sharing)”, in T.W. BYNUM, M. CALZAROSSA, I. DE LOTTO, S. ROGERSON (ed.), “Living, Working and Learning Beyond Technology”, *Proceedings of the Tenth International Conference Ethicomp 2008*, Mantova, University Press, 2008, pp. 211-223.

<sup>13</sup> See on this point U. PAGALLO, “Something Beyond Technology: Some Remarks On Ignorance And Its Role In Evolution”, in T.W. BYNUM, M. CALZAROSSA, I. DE LOTTO, S. ROGERSON (ed.), “Living, Working and Learning Beyond Technology”, *o.c.*, pp. 623-631.

irresponsive and incapable of communicating, learning, or memorizing. But what we still experience as the world offline is bound to become a fully interactive and responsive environment of wireless, pervasive, distributed, *a2a* (anything to anything) information process, that works *a4a* (anywhere for anytime), in real time. This will first gently invite us to understand the world as something ‘alive’ (artificially live). Such *animation* of the world will, paradoxically, make our outlook closer to that of pre-technological cultures which interpreted all aspects of nature as inhabited by technological forces”;<sup>14</sup> b) *from the real world to the virtual reality*: in this context, the concept of virtuality is endowed with a real content constituted by the idea of reliance on information. We have thus to shed light on this idea with regard to its pragmatic and gnoseological relevance. Reliance on information is a condition for a rational theory of decisions and actions. In order to decide or behave on the basis of rational criteria, I rely upon information: they are sensory data from reality (worldly ontology) or the content of knowledge (documental ontology) or instructions to behave (rules of conduct). According to Floridi, we can speak of information as reality; information on reality and information for reality.<sup>15</sup> Deciding and acting on the basis of reliable information has (a) the pragmatic aim of rationally guiding our decisions or actions toward a determined goal (according to a degree of probability of success) and (b) the gnoseological aim of measuring our decisions and actions by reference with an assumed parameter given by available information. Providing decisions and actions with a set of information implies giving supplementary information to the system (in terms of positive or negative feedback): this information has both descriptive (the conditions of reliance) and normative content (the degree of coherence between information and the results of decisions or actions).<sup>16</sup> The role of law as a mediation between the virtual and the real thus requires a more accurate analysis of the following conditions.

<sup>14</sup> See L. FLORIDI, “A look into the future impact of ICT on our lives”, *o.c.*, p. 7.

<sup>15</sup> The tripartite epistemological distinction of information can be found in L. FLORIDI, “Trends in the philosophy of information”, <http://www.philosophyofinformation.net>, p. 8. For an analysis of such a distinction and its relevance to law see U. PAGALLO, *Teoria giuridica della complessità. Dalla ‘polis primitiva’ di Socrate ai ‘mondi piccoli’ dell’informatica. Un approccio evolutivo*, Torino, Giappichelli, 2006, pp. 160-165.

<sup>16</sup> See on this point M. DURANTE, “What Model of Trust for Networked Cooperation? Online Social Trust in the Production of Common Goods (Knowledge Sharing)”, in T.W. BYNUM, M. CALZAROSSA, I. DE LOTTO, S. ROGERSON (ed.), “Living, Working and Learning Beyond Technology”, *Proceedings of the Tenth International Conference Ethicomp 2008*, *o.c.*, p. 212.

### 1. *From the virtual reality to the real world*

Law displays its role of mediation from the virtual reality to the real world, by endowing the virtual reality with a real content that is able to be appraised in the physical domain. This happens by means of *terms of legal responsibility*: it is within the real world that I am responsible for (the effects of) actions displayed within the virtual reality. In other words, legal responsibility is meant to measure the friction that an action or operation performed through computers in the virtual reality generates out of the domain of its technological application.

The virtual reality is a representation (either by analogical or digital models) of reality through which some objects are substituted by some other 'objects'. In this perspective, the virtual reality is an autonomous reality since the new objects, which design a reality with an economy of means or with a novel arrangement of them, produce a new form of knowledge.<sup>17</sup> The relation with the virtual reality is established by means of intuition (visual, acoustic perception of the new objects), conceptualisation (appraisal of the content of the new objects) or interaction (modification of the new objects by means of interactive technological devices). These types of relation are based on a specific epistemology, which does not explain what the virtual reality is but how it can be experienced and conceptualised by an epistemic agent at a given level of abstraction. This form of knowledge is necessarily and progressively elaborated on the basis of the sets of data (the new objects), which structure the *context* of the virtual reality: this context allows us to say that we behave and act *within* the virtual reality. In this perspective, how can we say whether and when the effects of an action performed within the virtual reality encounter the real world?

Coming back to the real world is only made possible out of the forms of relation with the representation of the (virtual) reality. Coming back to the real world requires translating the acquired knowledge within the epistemological realm where the effects of the actions displayed within the virtual reality are to be appraised and judged. One of the possible situations in which the effects of an action performed within the virtual reality encounters the real world is given by the factual circumstances where one is held responsible by someone else for those consequences within the real world. For one to be held responsible, it is required that the consequences of one's actions performed within the virtual reality were to some extent *foreseeable* within the epistemology describing how the real world can be experienced and conceptualised by an epistemic agent at a given level of abstraction. In such a perspective, law is entrenched with the

---

<sup>17</sup> See C. CADOZ, *Les réalités virtuelles*, Paris, Flammarion, 1994, p. 93.

epistemic role of appraising in what terms the effects of an action performed in the virtual reality can be judged foreseeable and thus accountable in the real world. This requires the legal science to establish the conditions of the representation of one term within the epistemological realm of another one. The foreseeable effects of an action are to be appraised in *terms of legal responsibility*. This does not mean that legal categories immediately apply to the technological reality nor it means that the virtual reality regulates itself by means of technological devices. On the contrary, according to the aforementioned Moor's thesis, it means that, when technology concerns the question of prediction, law is entrenched with the epistemic role of explaining how the consequences of an action can be experienced and conceptualised, in legal terms, as *foreseeable effects* both in the virtual and in the real world.

Needless to say, in our opinion the role of mediation is mainly worked out by means of legal adjudication, which not only consists in hearing and settling a case by judicial procedure but also in stabilising epistemic expectations, which mediate between the virtual and the real world. This aspect of the role of mediation of law poses both a phenomenological and a hermeneutical problem.

From a phenomenological point of view, the progressive convergence of online and offline life displaces the concept of prediction, which is no longer entrenched exclusively with the aim of inferring a future behaviour from a past one, but is also more and more concerned with the attempt of appraising the cognitive limits of the agents' representation of reality and of their rational capacity of acting,<sup>18</sup> which can enable us to correct our own predictions and to judge what can be held as a reasonable expectation.

---

<sup>18</sup> See G. SARTOR, "Gli agenti software: nuovi soggetti del cyberdiritto", <http://www.cirsfid.unibo.it/>, 2007, p. 81: "La conoscenza dei principi del funzionamento dell'agente e l'analisi del suo comportamento nel passato (l'agente può aver commesso errori) non offrono una base sufficiente per effettuare una previsione del suo comportamento futuro. Tale conoscenza può invece consentire di determinare i limiti delle capacità 'razionali' dell'agente, e quindi di individuare le ipotesi nelle quali l'agente può comportarsi in modo inadeguato. Combinando l'ipotesi della razionalità dell'agente con la conoscenza dei limiti di tale razionalità, siamo in condizione di prevedere e spiegare il comportamento dell'agente con sufficiente accuratezza. Non è diversa la strategia che adottiamo di regola nei confronti dei nostri simili: la nostra conoscenza dei limiti, delle idiosincrasie, delle attitudini di ciascuno non offre una base sufficiente per prevedere il comportamento altrui (tranne che nel caso di comportamenti dettati da riflessi automatici o da pulsioni incontrollabili). Tale conoscenza ci consente però di integrare e correggere l'ipotesi che ciascuno tenda a perseguire i propri scopi in modo razionale: possiamo spiegare e prevedere il comportamento umano combinando l'ipotesi generale della razionalità di ciascuno con la conoscenza dei limiti di tale razionalità nei singoli casi".

However, the progressive convergence of online and offline life does not displace the function of law, since there is still a difference between what is empirically held as a foreseeable effect and what is legitimately expected to be held, at an inter-subjective level, as a foreseeable effect.

From a hermeneutical point of view, the role of mediation of law by means of legal responsibility faces a different problem. In the ontology based on the physical reality the terms of legal responsibility are expected to be interpreted either within the context where the action took place or within the context where the action displayed its own effect (they often happen to be the same or at least to be both regulated by international law). What is the semantic context within which the actions or the effects of actions are to be legally interpreted within the networked society of information? The problem is not only concerned with legal boundaries (with the limits of both public and private international law) but also with symbolic universes: this is, in our opinion, the main problem that law has to face in its role of mediation between the real and the virtual, since data, phenomena, concepts, categories and the consequences of actions displayed within the virtual reality are likely to be culturally appraised in terms that refer to different symbolic universes.<sup>19</sup> The activity of mediation, by means of which one term can be represented within the epistemological realm of another one, presupposes, as we said, the possibility of a complex relatedness among data, that is to say, a unified

---

<sup>19</sup> See in this perspective S. MCROBB, Y. ORITO, K. MURATA, A. ADAMS, "Towards an Exploration of Cross-cultural Factors in Privacy Online", in T. WARD BYNUM, S. ROGERSON, K. MURATA (ed.), *Glocalisation: Bridging the Global Nature of Information and Communication Technology and the Local Nature of Human Beings*, vol. II, Global e-SCM Research Centre, Tokyo, Meiji University, 2007, pp. 380-385, at p. 381: "Most organizations and citizens in this domain share, due to their common linguistic and/or cultural heritage, assumptions that may not exist in non-Western cultures. Or, if they exist at all, they make take very different forms. By contrast, relatively little attention has yet been paid to the different meanings, values and behaviours associated with privacy in societies whose cultural compass points elsewhere than West". In the same perspective see also Y. ORITO - K. MURATA, "Rethinking the concept of information privacy: a Japanese perspective", in T. WARD BYNUM, S. ROGERSON, K. MURATA (ed.), *Glocalisation: Bridging the Global Nature of Information and Communication Technology and the Local Nature of Human Beings*, vol. II, *o.c.*, pp. 448-455, at p. 454: "Our proposal is made from a Japanese perspective. This may raise concerns about the effectiveness of the revised concept in the global context. However, because ICT is advancing on a global scale, the revised concept could become mandatory for a wide range of countries. Our proposal is the first step towards developing a globally acceptable concept of the right to information privacy that is appropriate for the modern information age. Societies could realise this concept through the integration of opinions about the right to such privacy based on local sociocultural and economic situations".

symbolic universe. In addition to this, we should notice that the development of the semantic web and formal ontology is an important but only partial answer to the problem, since this development mainly aims at coping with the interpretation of (legal) texts rather than with the present delimitation of (legal) contexts. While the information and communication technology (ICT) is advancing on a global scale, the role of mediation of law appears to be, often, linguistically and/or culturally located.

## 2. *From the real world to the virtual reality*

Law displays its role of mediation, furthermore, from the real world to the virtual reality, by giving a real content to the real world that can be appraised within the virtual reality, by means of *informational reliance*. It is within the virtual reality that I rely on informational data, in order to perform actions that are likely to produce (legal) effects within the real world. In other words, if the virtual dimension of information and communication technology (ICT) is to be found in its ability to transform the world in the content of an information, the virtual dimension of law (as a mediation from the real world to the virtual reality) is to be found in its ability to set the conditions according to which it is possible to rely on the content of information processed and exchanged within the networked information society. In order to rely upon information, epistemic agents have to either explicitly or implicitly set a *norm* which should allow them to recognise intersubjectively what is reasonable to believe in and expect. In the absence of such normative dimension, the communication spread in the networked information society is radically exposed to the chance of being disordered and ineffective.

In this perspective, law can play a fundamental role of mediation between the real and the virtual to the extent that it assures reliance upon information. This does not amount at saying that the virtual reality of the networked information society should be subject to ruling: in this line of reasoning, the mediation of law is called forth only by reference to its normative function of stabilisation of expectations. This aspect of mediation poses topological problems both with respect to (1) *information and communication technologies* and with respect to (2) *networked cooperation*.

### a. Information and communication technologies

In relation to information and communication technologies (ICT) the *function-of-law* consists (a) in creating *filters of relevance and reliability*, in order to select relevant and reliable information (data and channels of information), and (b) in establishing *means of moderation and meta-moderation*, in order to ensure an ordered communication, without reaffirming forms

of control after decentralisation.<sup>20</sup>

*Filters of relevance and reliability*

Communication in the networked information society has to be ordered<sup>21</sup> to be effective. This requires to elaborating means by which it is possible to filter information in terms of relevance and reliability. Needless to say that the creation of filters of relevance and reliability is likely to suffer from problems of agency, *i.e.* any selection is by itself significant and thus possesses the normative power of conveying (more or less perceptible) values.

However, the elaboration of these filters in the networked information society does not depend necessarily on centred and hierarchical choices (related to the ownership of channels of information). On the contrary, it has been proved<sup>22</sup> to depend on decentred and horizontal practices displayed by a plurality of users by means of distributed networks.<sup>23</sup> More precisely, there are at least two ways to create filters of relevance and reliability through the coordination of individual actions. This coordination can be either the result of the users' *cooperative will* or the outcome of their *spontaneous interaction*.

Internet users can voluntarily create means by which information is judged as relevant and reliable thanks to an assessment that has been progressively formed by the pronounces and/or the practices of a plurality of individuals, whose interaction allow them to reach a goal they would not be able to achieve by themselves. This is made possible by all technological filters of relevance and reliability created, in a distributed manner, in accordance with a *teleological hierarchy*. I define as such a hierarchy of values, the ordering of which is constructed with the scope of achieving a previously

<sup>20</sup> For a detailed analysis of this question, R.A. GALLOWAY, *Protocol. How Control Exists after Decentralization*, Cambridge (Mass.), MIT Press, 2004. See also R.A. GALLOWAY & E. THACKER, *The Exploit: A Theory of Networks*, Minneapolis, University of Minnesota Press, 2007.

<sup>21</sup> The idea has been defended against criticism in M. DURANTE, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete, o.c.*, pp. 259-273.

<sup>22</sup> See in this perspective, Y. BENKLER, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, New Haven, Yale University Press, 2006, pp. 215-220.

<sup>23</sup> For a critical account of this notion see R.A. GALLOWAY & E. THACKER, *The Exploit: A Theory of Networks, o.c.*, p. 3: "In contrast to Lovink, we maintain that in recent decades the process of globalization have mutated from a system of control housed in a relatively small number of power hubs to a system of control infused into the material fabric of distributed networks".

shared goal of a common concern.<sup>24</sup>

Internet users can, furthermore, elaborate filters of relevance and reliability as a result of a non-programmed action, that is to say in a spontaneous manner (cosmological order).<sup>25</sup> In this case, the coordination of individual actions is made possible by the specific configuration of networked interactions (according to topological models<sup>26</sup> that we cannot expound here), which tend to select information both in a relevant and ordered way. This process of selection is based on clusters of shared contents, common interests, and the presence of hubs, which filter and catalyse the informational resources distributed in the web. On the one hand, this may result, at a macroscopic level, as a *non-democratic*<sup>27</sup> distribution of information (*power law distribution*: very few websites has the majority of links and the majority of websites has very few links). On the other hand, this means that communication is made possible, at a regional level, since information is guided towards local communities by interests of common concern, as it is described by the topological effects of clustering, cross-linking and small worlds.<sup>28</sup>

#### *Means of moderation and meta-moderation.*

<sup>24</sup> For such an idea see M. DURANTE, *Il futuro del web: etica, diritto, decentramento. Dalla sussidiarietà digitale all'economia dell'informazione in rete*, o.c., p. 201: "[...] se di gerarchia si può ancora parlare, preferiamo allora qualificarla come *gerarchia orientata ad un fine comune*: è l'orientamento alla protezione del fine comune che designa il principio di misura e legittimità dell'atto d'autorità insito in ogni processo di revisione e accreditamento, per quanto esso sia orizzontale e decentrato".

<sup>25</sup> The idea of a cosmological order has been suggested by F. HAYEK, *Law, Legislation and Liberty*, London, Routledge & Kegan Paul, 1982.

<sup>26</sup> See on this note n. 28. See also R.A. GALLOWAY & E. THACKER, *The Exploit: A Theory of Networks*, o.c., p. 13: "By 'thinking topologically', we mean an approach that compares the abstract spaces of different structural or architectonic systems. Pyramidal hierarchy and distributed networks, for examples, have two different topologies of organizations and control".

<sup>27</sup> See on this point A.L. BARABÁSI, *Linked*, Cambridge, Perseus Edition, 2002. See also C. SHIRKY, "Power Laws, Weblogs, and Inequality", [http://www.shirky.com/writings/powerlaw\\_weblog.html](http://www.shirky.com/writings/powerlaw_weblog.html).

<sup>28</sup> For an account of networked topological effects, Y. BENKLER, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, o.c., pp. 300-320. On the topological configuration of small worlds paradigm see in particular, D.J. WATTS – S.H. STROGATZ, "Collective dynamics of 'Small-World' Networks", in *Nature*, 393, 1998, pp. 440-442; D.J. WATTS, *Small Worlds: The Dynamics of Networks between Order and Randomness*, Princeton, Princeton University Press, 1999; see also U. PAGALLO, "'Small world' paradigm in social sciences: problems and perspectives", in T. WARD BYNUM, S. ROGERSON, K. MURATA (ed.), *Glocalisation: Bridging the Global Nature of Information and Communication Technology and the Local Nature of Human Beings*, o.c., vol. II, pp. 456-465.

Communication in the networked information society implies inter-subjective interactions, which need to be moderated, in order to enable users to equally and fruitfully participate in the community of discussion. In this perspective, the *function-of-law* consists in establishing means of moderation, *i.e.* the social norms regulating the discussion, and metamoderation, *i.e.* the social norms regulating how the norms of discussion are to be chosen and applied.

We consider a community of discussion,<sup>29</sup> which does not adopt a process of selection of information that makes, *ex ante*, a distinction between what can be published and what has to be prevented from publishing. The process of publishing is based on an *ex post* peer review system of selection. This means that this community endorses both a principle of freedom and a principle of responsibility: the former asserts each participant's freedom to post whatsoever information, the latter requires the participants to establish shared means of moderation and metamoderation, in order to revise information.

The process of moderation, adopted by the community of discussion, is decentred and horizontal, as it is based on the distributed power of evaluation of each moderator selected by the community. Even if distributed, this normative power has to be subject to further control by means of metamoderation, which is also a decentralised and horizontal mechanism of revision. The concept of metamoderation consists in the idea that every judgement should be subject to further judgement. This does not necessarily entail an infinite regression, since metamoderation is implicitly judged by its ability to determine a fruitful and ordered discussion within the community.

The *legal constitution* of such a community deserves consideration. The community is neither constituted exclusively on inclusion nor does it on exclusion. Its constitution endorses both a norm including every statement in the discussion and a norm excluding some of them from there. The community does not formulate a judgement on what is included but asserts a judgement on what is excluded. This means that the community is not involved in the process of deciding what can be a priori conceived as *just*, but is indeed concerned with the process of establishing what can be a posteriori conceived as *unjust*, that is to say that cannot be accepted within

---

<sup>29</sup> We consider the example of moderation and metamoderation offered by the multilevel technological platform adopted by a community of discussion as Slashdot. See on this point D. TAPSCOTT –A.D. WILLIAMS, *Wikinomics: How Mass Collaboration Changes Everything*, New York, Portfolio, 2006, pp. 144-145.

the discussion.<sup>30</sup>

b. Networked social cooperation

Networked social cooperation not only requires to relying on the information of others when deciding or behaving under the conditions of uncertainty resulting from the complexity of virtual environment, but also on someone's else behaviour (delegation). This raises a normative question as regards interpersonal interaction: must interaction be based on a previously established norm, in order to promote cooperation? Or is such a norm likely to grow out of the interpersonal interaction? Before trying to answer such a question, we should focus our attention upon the fact that the idea of establishing a norm regulating the interpersonal interaction already implies a certain degree of distrust (in the relations between agents).

The computer-mediated interaction or coordination between agents or groups may require thus different forms of normative mediation, either founded upon (a) distrust systems of mediation or upon (b) trust systems of mediation. The former is mainly concerned with technological and legal security (assured by means of rules, constraints, architectures, controls, and protocols), while the latter is mainly concerned with mental and social dispositions towards other agents.<sup>31</sup> Technological or legal security is necessary in regards to online commercial transactions, privacy issues, and legal contracts, but it does not suffice to assure networked social cooperation. In fact, this is based on someone else's behaviour, on their willingness to cooperate with us that is never fully predictable. A trust system of mediation allows the trustier to evaluate the trustee's willingness and ability to fulfil expectations.

*Distrust systems of mediation.*

Internet users set norms or technological devices since they do not trust the agents to whom they delegate tasks. This system shows a negative attitude towards agents, since it applies when they do not fulfil expectations. When things are expected to go wrong, there is no particular concern for the goal to achieve. This system externalises concern for the goal, whose protection and fulfilment are attributed to a third party

<sup>30</sup> See in this perspective, even tough in the context of a different line of reasoning, what has been affirmed by P. RICŒUR, *Le juste*, Paris, Esprit, 1995.

<sup>31</sup> This perspective has been widely expounded by C. CASTELFRANCHI & R. FALCONE, "Social Trust: Cognitive Anatomy, Social Importance, Quantification and Dynamics", *Proceedings of the first Workshop on Deception, Fraud and Trust in Agent Societies*, Minneapolis/St. Paul, 1998, pp. 35-49. More recently, see also of the same authors, "Trust Theory", 2007, <http://www.istc.cnr.it/T3/trust>, and "Socio-Cognitive Model of Trust: Basic Ingredients", 2008, <http://www.istc.cnr.it/T3/trust>.

(normative mediation): the authority. This consists of two elements: a) the norm (legal rules or technological devices) set before the trustier and the trustee enter into a relation; b) the institution that administers and applies the norm established to regulate the relation between parties. The system based on distrust is ultimately based on trust, since the trustier has to trust the ability of the norm to foresee when the agents will not fulfil expectations and, above all, the ability of the authority to apply the violated norm. This normative mediation entails high transaction costs<sup>32</sup> in setting up an institutional authority to be trusted and feared and applying the norms regulating the interpersonal interaction.

*Trust systems of mediation.*

The trustier believes that the trustee will act according to predictions. This system internalises concern for the goal. A positive attitude is motivated by the Internet users' shared concern for the task to be fulfilled. This model applies when the desired outcome is produced. This system does not seem to refer to an institutional authority (normative mediation). However, it is a relationship based on a particular type of authority. This consists of two elements: a) the social norm set by the relation between agents. Trust itself sets a norm that grows out of the dynamic sphere of the communication process (interpersonal interaction): both the trustier and the trustee are aware of the fact that the latter is somehow indebted to the former, since the trustier has given the trustee some credit;<sup>33</sup> b) information concerning the trustee's behaviour. The act of trusting and the act of fulfilling expectations release mutual information that can be shared and processed within the web or a community (the system in relation to the virtual environment). The authority of trust lies in the possibility of tracking and sharing this information. It is a form of control

---

<sup>32</sup> P. AIGRAIN, "The Individual and the Collective in Open Information Communities", *Proceedings BLED Electronic Commerce Conference*, 9-11 June 2003, <http://paigrain.debatpublic.net>: "Transaction costs are much more than the monetary costs attached to transaction. They include cognitive costs (for instance the cost of deciding whether or not to do an action that may lead to a charge), time and information costs (for instance navigating in the transaction management layers), privacy costs, uncertainty costs (when some rights are subject to further approval), locking-in (*i.e.* loss of freedom due to the fact that an information service will give you access only to specific sources, or will make it difficult for you to switch to another provider). In this sense [...] control aspects are more rejected than the cost itself".

<sup>33</sup> See N. LUHMANN, "Trust: a mechanism for the reduction of social complexity", in ID., *Trust and Power: Two Works by Niklas Luhmann*, New York, John Wiley & Sons, 1979, pp. 1-103, at p. 35, who affirms that the trustor "has the possibility to set the norm according to which his reliance should not be betrayed (...). The impossibility of enchaining trust within a legal disposition does not entirely exclude trust from the domain of norms".

by means of *information feedback*: negative feedback corrects an incorrect prediction; positive feedback supports the process of communication.

A trust system of mediation, built as a result of relations between agents and the stabilisation of their mutual expectations, determines a normative dimension that can reach beyond technological and legal security, since it is not affected by obsolescence (because it grounds expectations on the ongoing conditions of party relations) nor does it require full information (because it enables agents to deal with conditions of uncertainty and lack of knowledge), and thus high transaction cost, in order to be established.

## V. CONCLUSIONS

The theoretical framework – within which we have analysed in what sense law can devise an act of mediation which determines the conditions of possibility of the representation of what is referred to as ‘virtual reality’ within the realm of what is referred to as ‘physical reality’ and vice versa – is thus structured by the *inter-subjective* computer-mediated interaction and communication between individuals or groups. The rationality of the interaction between agents (whether human or artificial) is not actually defined in terms of certainties or acquired knowledge but rather in terms of shared expectations and social norms, which grow out of the communication process.

The rational criteria of inter-subjective interaction have been settled thanks to the mediation of law along two directions: on the one hand, law is entrenched with the role of devising how to protect reliance on information, which assures an ordered form of communication between agents, by qualifying what is conceived as reliable information by means of legal responsibility. On the other hand, law is concerned with setting the conditions of the communication process, by means of which agents can devise what is reasonable to expect from other agents, both in terms of relevant and reliable information (filters and means of moderation and metamoderation) and in terms of trusting delegated tasks and behaviours (networked cooperation).

In both perspectives, the relation between agents can be judged as an inter-subjective interaction, since the parties are transformed by the interaction itself. To speak more properly, the communication process constitutes the parties in their own subjectivity. Whether human or artificial, subjectivity is conceived in epistemological terms as the ability to set the criteria assessing how (virtual and physical) reality can be experienced and conceptualised at a given level of abstraction. Since this ability grows out of the communication process, it is not possible to

determine, as a fixed certainty, what is to be taken for stable: the shared basis of our decisions and behaviours is the result of the reduction of complexity of the environment. The act of mediation of law between the real and the virtual plays a role in the process of reduction of complexity, which is not to be underestimated, if the interplay of intuitions (the phenomenon to be represented: factual question) and concepts (the conditions of possibility of representation: legal question) deserves to be preserved.

## NEW TECHNOLOGIES AND THE LAW: PRECEDENTS VIA METAPHORS

Harmeet Sawhney, Venkata Ratnadeep Suri, and Hyangsun Lee\*

### I. INTRODUCTION

In many ways it is futile to think about the future. There are far too many variables involved and it is almost impossible to make accurate predictions. But, in the arena of information and communications technologies (ICT), the sheer pace of technological change forces us to confront it. We have to factor in the future when we make investment, regulatory, and other decisions about ICT.<sup>1</sup>

The preferred device is a formal model which allows us to make predictions with a high degree of accuracy. Such a model requires a comprehensive understanding of the phenomenon and availability of accurate data. Unfortunately, the sheer complexity of the processes leading to the development of a large technical system such as the “information superhighway” does not readily lend itself to precise modelling. The processes tend to be ambiguous and ill-defined and accurate data are a rare commodity. In such situations metaphors and analogies offer a viable alternative to formal models. They help us handle situations where there is “high uncertainty, missing data, unclear goals, and poorly understood parameters”.<sup>2</sup>

We have to accept the fact that although the use of metaphors is not a particularly elegant or sophisticated technique, it is perhaps the only conceptual tool we have for understanding the development of a new technology. We should therefore direct our energies towards understanding the peculiarities of this tool: How can we leverage it to maximise the potential payoff? What are the pitfalls and how can we avoid them?

In the case of technology and law, there is an added dimension—metaphors help establish precedents. As Pool points out, “courts like to

---

\* Department of Telecommunications, Indiana University, Bloomington.

Endnotes

<sup>1</sup> The introductory discussion excerpts from H. SAWHNEY, “Information Superhighway: Metaphors as Midwives”, *Media, Culture & Society*, 1996, No 18, pp. 291-314.

<sup>2</sup> G. KLEIN, “Applications of Analogical Reasoning”, *Metaphor and Symbolic Activity*, Vol 2, Issue 3, pp. 201-218, 1987, at p. 202.

treat new phenomenon by analogy to old ones”.<sup>3</sup> For example, in the mid-1970s when FCC removed the resale restrictions on telephone services, “the fundamental legal principle underlying the decision was a 1911 Supreme Court decision which prohibited the railroads from refusing service to freight forwarders who purchased railroad service in bulk (carload lots or greater) and resold it to smaller shippers”.<sup>4</sup> This mode of legal reasoning has formed the basis for the development of much of the communications law. Each new communications technology has been shaped by legal precedents created by the previous ones.

The problem is that the precedents are often not readily available or clear. The Interstate Commerce Act developed for regulating the railroads has continued to influence the development of the legal framework for all the subsequent network technologies—petroleum pipelines, trucking, civil aviation, and telecommunications, among other technologies. Here metaphors were effective vehicles for the transfer of conceptual frameworks from one technology to another because they were all point-to-point networks for the movement of materials and information from one point to another. However, the process broke down in the case of radio. For example, in the beginning radio was conceptualised as “wireless telegraph” or a point-to-point communication technology. Even Marconi, the inventor of radio, saw the tendency of radio waves to scatter as a major nuisance. In fact all the institutional forces guided by the telegraph analogy were working in the 1920s towards casting radio as a point-to-point technology. The eventual emergence of broadcasting was a total surprise, and it undermined all the institutional structures set up on the wireless telegraph metaphor. The radio was clearly a case where a metaphor based on an old technology failed to shape the new one in its image.

The development of broadcasting created what we call a “metaphor vacuum”—there were no readily available metaphors to think about the new technology. The term “broadcasting” was appropriated from a realm far removed from communication. The original meaning of broadcasting signified the act or process of scattering seeds.<sup>5</sup> Later, at the turn of the century, the women suffragists used the word broadcasting to describe the act of distributing leaflets on street corners.<sup>6</sup> This mode of disseminating

---

<sup>3</sup> I.D.S. POOL, *Technologies of Freedom*, Cambridge, MA, Harvard University Press, 1983, at p. 100.

<sup>4</sup> G. BROCK, *The Telecommunications Industry*, Cambridge, MA, Harvard University Press, 1981, at p. 270.

<sup>5</sup> E. BARNOUW, *A Tower in Babel*, New York, Oxford University Press, 1994.

<sup>6</sup> J. HIJIYA, *Lee de Forest and the fatherhood of radio*, Cranbury, NJ, Associated University Press, 1992.

something came closest to serving as an analog for describing the dispersive tendencies of radio.

Although “broadcasting” was an appropriate label for the new phenomenon, it was not very useful from the legal point of view, which is the focus of our paper. It described the physical phenomenon—point to multipoint communication. But it did bring with a legal framework. We are interested in understanding how the legal system dealt with the central problematic of the “metaphor vacuum.” Here, on the one hand, there was a radically new technology for which no clear precedent was available. On the other hand, the case law could not proceed without a precedent. The one way this tension could be resolved was by taking an established metaphor and stretching it. We are especially interested in understanding how this stretching process works.

In this paper we first trace the legal developments from the very first case—*Marconi Wireless Telegraph vs. Northern Pacific S.S. Co.* (1918) to *Great Lakes Broadcasting vs. Federal Radio Commission* (1930), when the framework for radio regulation became a settled issue. In the subsequent section we analyse the radio case on a conceptual plane and draw lessons for the future.

## II. EVOLUTION OF RADIO LAW AND REGULATION

The initial cases dealt with minor issues. For example, the earliest court case we found, *Marconi Wireless Telegraph vs. Northern Pacific S.S. Co.* (1918), was primarily a contract dispute between two parties. At this stage, the potential for broadcasting was not well understood. Wireless was basically being used in ways that mimicked the telegraph.<sup>7</sup> Consequently, the issues

---

<sup>7</sup> Edison mimicked gas to get electricity, which was then a radically new technology, accepted by consumers and thereby gain a toehold in the marketplace. Aware that interior lighting generated 90% of the revenue of the gas industry, Edison poured his energies into developing a small 16 candle-power electric light (equivalent to the standard gas jet of 1880s) that would be appropriate in doors. In Edison’s own words, as he noted in his notebook, “Object. Edison to effect exact imitation of all done by gas so as to replace lighting by gas by lighting by electricity . . . Edison’s great effort not to make a large light or a blinding light but a small light having the mildness of gas.” (H.C. PASSER, *The Electrical Manufacturers 1875-1900*, Cambridge, MA, Harvard University Press, 1953, at p. 82).

Also see (H. SAWHNEY and X. WANG, “Battle of Systems: Learning From Erstwhile Gas-Electricity and Telegraph-Telephone Battles”, *Prometheus*, 2006, Vol 24, No. 3, pp. 235-256) for a more complete description of how Edison mimicked gas. Also see (D. LEONHARDT, “A Voice in the Calling Wilderness”, *New York Times*, 18<sup>th</sup> Dec. 2003, p. E1) for a discussion on how Internet phone service providers are piping in fake dial tone to make the new technology feel familiar.

it raised were relatively minor, as opposed to paradigm shifting. The ambiguity was low.

Subsequently, the cases started getting more complex. With increasing number of actors, new issues started emerging, such as copyright violations, jamming, etc. The earliest set of radio court cases—*M. Witmark & Sons v. L. Bamberger & Co.* (1923), *Pastime Amusement Co. vs. M. Witmark & Sons* (1924), and *Jerome H. Remick & Co. vs. American Auto Accessories Co.* (1925) —involved copyright infringement and primarily concerned broadcast of music through radio.<sup>8</sup> In all these cases broadcasters contested copyright infringement allegations, arguing that their broadcasts of live concerts were not “for profit” as they did not charge their audiences. Similarly, broadcasters also argued that their broadcasts were not “public” as they were received in the privacy of their audiences’ homes. The courts, however, rejected these arguments in favour of the plaintiffs stating there was infringement of music copyrights because a performance by an artist for radio broadcast is “consciously addressing a great, through unseen and widely scattered audience”.<sup>9</sup> The second set of early court cases involved re-broadcasting of radio music over closed circuit audio systems in hotels. One early case, *Buck vs. Jewell LaSalle Realty Co.* (1931) is particularly illustrative of this.<sup>10</sup> In this instance too, Justice Brandeis, commenting on the innovative ways in which radio broadcasting technology was being exploited, remarked that, “while this (form of exploitation) may not be possible before the development of radio broadcasting the novelty of the means used does not lessen the duty of the courts to give full protection to the monopoly of public performance for profit which Congress has secured to the composer”.<sup>11</sup>

On parallel lines there was also an increasing realisation that the commerce clause alone was not adequate for regulation of radio since it gave the government ability to only issue licenses to operate but not actually regulate behaviour.

In the beginning radio was regulated on the basis of the Commerce Clause of the Radio Act of 1912. The Department of Commerce argued that since radio waves transcended state boundaries and radio broadcasting was a commercial activity, radio could be regulated on the basis of the commerce clause. Here the analogies were the telegraph and the telephone, where transmission of messages by electronic means had been construed to be

---

<sup>8</sup> J.C. GINSBURG, “Copyright and Control over New Technologies of Dissemination”, *Columbia Law Review*, 2001, Vol. 101, No. 5, pp. 1613-1647.

<sup>9</sup> *Ibid.*, at p.1620.

<sup>10</sup> *Ibid.*

<sup>11</sup> *Ibid.* at 1621.

interstate commerce.<sup>12</sup> The case of *Whitehurst vs. Grimes* (1927), presents an interesting illustration of the application of the commerce clause to the field of radio communication. The plaintiff operated a radio station in the city of Wilmore in Kentucky, under license from the Secretary of Commerce. The city of Wilmore passed an ordinance requiring all persons operating a radio station to pay a tax to the city and imposed a penalty for failure to do so. In its decision the court held that radio was inherently an interstate commercial activity and hence the ordinance by the city of Wilmore was void given that Congress had placed radio under the purview of the commerce clause.<sup>13</sup>

While the commerce clause became the basic framework for radio regulation, there was increasing uncertainty about its legal basis. For example, in a legal review article, C.K.U (1928) challenged the application of the commerce clause to radio broadcasting.

“Today, however, by far the larger part of radio broadcasting consists of music and other entertainment distinguishable in many respects from the conveyance of commercial messages. The act makes no distinction and its administration has included both types. It would seem that here the arguments in the telegraph and telephone cases, that those companies were “agencies in interstate commerce” or “common carriers of messages” among states, would be scarcely applicable. Indeed, such broadcasting is more like a free band concert on one side of a state line being enjoyed by the public on the other side. If the state in which the band was playing undertook to regulate its time and place of playing, would such state be interfering with interstate commerce”...[ ] “Is a man who places a large advertising sign on one side of a state border engaged in interstate commerce because it can be seen across the line? Yet the act extends its operation to pictures sent through the air by radio”.<sup>14</sup>

At the same time, the advancement of radio and aviation technologies had started a debate among legal experts who stressed the increasing need for laws regulating the usage of air space. An interesting point of view emerged in conferences and publications that the air above an individual's property must be treated as that individual's property and the government must make laws that regulate the proper use of air space. With regard to radio broadcasting, there was increasing consensus among legal experts for the establishment of a federally controlled radio board for regulating the radio

---

<sup>12</sup> C.K.U, “The Radio and Interstate Commerce”, *Michigan Law Review*, 1928, Vol. 26, No.8, pp. 919-921.

<sup>13</sup> *Ibid.*

<sup>14</sup> *Ibid*, at p. 920-921.

industry's use of air space.<sup>15</sup>

Nevertheless, the commerce clause continued to be the basis for radio regulation until two land mark court decisions—*Hoover (Secretary of Commerce) vs. Intercity Radio Co.* (1923), and *Zenith Radio vs. United States* (1926), changed it all. In both these instances the Secretary of Commerce refused to renew broadcast licenses belonging to the plaintiffs who in turn initiated legal action challenging the legal basis for the denial of licenses. The courts ruled in favour of the plaintiffs arguing that the Secretary of Commerce had no discretion to refuse licenses.<sup>16</sup> These landmark court decisions “totally laid bare the absence of a legal basis” for regulation of radio broadcasting.<sup>17</sup>

The Radio Act of 1912 was largely conceived to function as a registry device for issuing licenses to all those who applied for one. However, the subsequent policies and actions pursued by the Department of Commerce were both allocative and regulatory in nature. The decision rendered in these two cases completely annulled the regularly role of the Department of Commerce by holding that “the Secretary of Commerce had no power to make regulation and was to issue licenses”.<sup>18</sup>

Once the potentiality of broadcasting was fully understood—it raised a whole new set of legal issues. With the court decision in *Zenith Radio vs. United States* rendering the Radio Act of 1912 and the Department of Commerce's legal authority over radio broadcasting virtually ineffective, radio broadcasting between 1926 and early 1927 was characterised by chaos and confusion.<sup>19</sup> Walter S. Gifford, President of Bell Telephone Company, noted “Nobody knew...where radio was really headed. Everything about broadcasting was uncertain”.<sup>20</sup> Recognising the fundamental deficiencies of existing regulatory tools, the then Secretary of Commerce convened four annual national radio conferences where he advocated the concept of “public interest” in radio communication. Subsequently, Congress passed the Radio Act of 1927 that led to the establishment of the Federal Radio

---

<sup>15</sup> BAR ASSOCIATION OF TENNESSEE, “The Law of the Air”, in *Proceedings of the 43rd Annual Session of the Bar Association of Tennessee*, 1998, Chattanooga, Bar Association of Tennessee, 1924, pp. 190-198.

<sup>16</sup> J.R. MINASIAN, “The political economy of broadcasting in the 1920's”, *Journal of Law & Economics*, 1969, Vol. 12, No. 2, pp. 391-403.

<sup>17</sup> Y. BENKLER, “Overcoming an agoraphobia: Building the commons of the digitally networked environment (wireless telegraph regulation)”, *Harvard Journal of Law & Technology*, 1998, Vol. 11, No. 2, pp. 287-400, at p. 316.

<sup>18</sup> J.R. MINASIAN, *o.c.*, at p.401.

<sup>19</sup> *Ibid.*

<sup>20</sup> J. BROOKS, *Telephone: The First Hundred Years*, New York, Harper & Row, 1976, at p.161.

Commission with broader powers to regulate radio broadcasting. The 1927 Radio Act employed a utility based regulation model under which broadcasters were deemed to be public trustees who were “privileged” to use a scarce public resource.<sup>21</sup>

After the passage of the Radio Act of 1927, a number of court decisions followed that firmly established Public Interest Convenience and Necessity (PICON) as the basis for radio broadcast regulation.<sup>22</sup>

In *Technical Radio Lab vs. Federal Radio Commission* (1929) the court reaffirmed Federal Radio Commission’s authority to limit access to airwaves where applicants outnumbered channels available (Le Duc & McCain, 1970). In a similar case *Carrell vs. Federal Radio Commission* (1929), the court affirmed the commission’s right to deny licenses to one particular class of operators in order to reduce interference.<sup>23</sup> *Great Lake Broadcasting Co. vs. Federal Radio Commission* (1930) was the next milestone in radio regulation. The case involved a conflict among three Chicago area broadcasters about modification of their technical facilities to minimise interference. In the process of accessing their claims, the court made nature and quality of content and its value to the community the station is serving as a basis for assessing the performance of a station under public interest standard. The Great Lakes Broadcasting decision is considered significant in the history of radio broadcasting as it set the precedent for content as a criterion for assessing public interest.<sup>24</sup>

### III. LESSONS FOR THE FUTURE

Most new technologies easily get beaded into the ongoing transfer of metaphors from one technology to another. The development of infrastructure networks—electric grids, highway systems, telegraph, railroad, and telecommunications networks—was marked by the transfer of frameworks from one technology to another. As noted earlier, the frameworks developed for the railroads were transferred to subsequent technologies, especially through the Interstate Commerce Act. Later, the deregulation of transportation industries in the 1970s set the stage for the

---

<sup>21</sup> E.G. KRASNOW and J.N. GOODMAN, “The ‘Public Interest’ Standard: the Search for the Holy Grail”, *Federal Communications Law Journal*, 1998, No. 50, No. 3, pp. 606-636.

<sup>22</sup> *Ibid.*

<sup>23</sup> D.R. LE DUC and T.A. MCCAIN, “The Federal Radio Commission in Federal Court: Origins of Broadcast Regulatory Doctrines”, *Journal of Broadcasting*, 1970, Vol. 14, No. 4, pp. 393-410.

<sup>24</sup> E.G. KRASNOW, and J.N. GOODMAN, *o.c.*

deregulation of the telecommunications industry in the 1980s.<sup>25</sup> More recently, we have been seeing the migration of deregulatory concepts from telephone regulation to electricity regulation, especially with regard to competition in local markets. These transfers tend to occur relatively fluidly because all these infrastructures are point-to-point networks that transport materials and information from one point to another. Metaphor vacuums occur when we are confronted with a radically new technology such as radio.

In this concluding section, using the radio case as a springboard, we conceptualise the processes that lead to the creation of a metaphor vacuum and also its eventual resolution. In specific we focus on: (1) when metaphor vacuums occur, (2) how they are resolved, and (3) how the metaphors used early in the process shape the possibilities down the line.

#### **IV. THE PROCESS LEADING TO THE METAPHOR VACUUM**

Even in the case of an unprecedented technology like radio, the metaphor vacuum does not occur right after the arrival of the new technology. The reason is that initially the new potentiality of the technology is not fully understood. In the early stages, the new technology is employed in ways that mimic old technologies. In our particular case, the radio was deployed as wireless telegraph. Accordingly, the cases that arise at this stage are of a relatively minor nature. As discussed earlier, *Marconi Wireless Telegraph vs. Northern Pacific S.S. Co.* (1918), the first case we found, dealt with a contract dispute between two parties. In general the ambiguity tends to be low in the initial cases because the new technology is used in old and familiar ways.

Later, as usage spreads, trial and error generates insights into new possibilities opened up by the new technology. These opportunities are capitalised on by various interests and the resulting cases are much more complex than the initial ones. Now, the ambiguity is significantly higher because the new usages do not simply mimic the old technologies but open up new and often unprecedented patterns of organisation and behaviour. In the case of radio, we had, on the one hand, the problem of applying old frameworks such as copyright and the commerce clause to a new mode of communication, and, on the other hand, the unprecedented problem of jamming. These complexities are dealt with by stretching the established metaphors and frameworks until a breaking point of sorts is reached which

---

<sup>25</sup> B. CHERRY, "Back to the Future: How Transportation Deregulatory Policies Foreshadow Evolution of Communications Policies", *The Information Society*, 2008.24, No. 5, pp. 273-291.

creates a metaphor vacuum or a realisation that we need a radically new framework.

## V. THE FILLING OF THE METAPHOR VACUUM

When a metaphor vacuum is generated, one would expect that a systematic process for identifying an appropriate metaphor would be in order. One such approach would be what Peirce (1931) calls abduction, wherein metaphors are treated as provisional hypothesis, which are held only as long as the facts permit. The following description of the process by which the researchers deciphered the Egyptian cuneiform descriptions illustrates abduction:

“In the first steps that were made toward the reading of the cuneiform inscriptions, it was necessary to take up hypotheses which nobody could have expected would turn out true,—for no hypothesis positively likely to be true could be made. But they had to be provisionally adopted,—yes, and clung to with some degree of tenacity too,—as long as the facts did not absolutely refute them. For that was the system by which in the long run such problems would quickest find their solutions”.<sup>26</sup>

But in reality the process is quite chaotic mainly because it unfolds amidst the cacophony of the political arena, as opposed to the deliberateness of a seminar room discussion. When the two land mark court decisions—*Hoover (Secretary of Commerce) vs. Intercity Radio Co.* (1923), and *Zenith Radio vs. United States*—set aside the commerce clause as the basis for radio regulation, there was need for another legal framework. According to Krasnow and Goodman (1998), the legislators, while deliberating the 1927 Radio Act, were groping for a standard that would spell out the obligations of the licensees. They were looking for something that was concrete enough to provide clarity for current needs and yet flexible enough to accommodate unanticipated uses of the technology in the future. Within this context, a chance conversation between Senator Clarence Dill and a young lawyer on loan from the Interstate Commerce Commission (ICC) provided the solution. The ICC lawyer suggested “public interest, convenience and necessity” (PICON) as a standard and it caught the senator’s imagination.<sup>27</sup> Thereby broadcasting ended up with a standard

<sup>26</sup> C. PEIRCE, “Pragmatism and Abduction”, pp. 112-127 in C. HARTSHORNE and P. WEISS (eds), *Collected Papers of Charles Sanders Peirce*, Vol. 1, 1931, Cambridge, MA: Harvard University Press, p. 142.

<sup>27</sup> E.G. KRASNOW and J.N. GOODMAN, *o.c.*

from the world of transportation systems and public utilities.<sup>28</sup> Le Duc and McCain note, the public interest standard meant “a revolution in practice, at least as to broadcasting . . . and with the exception of common carrier or utility matters, the idea of . . . public convenience as a condition for entry into interstate commerce was unique in Federal legislation”.<sup>29</sup> This choice had its consequences, as discussed later.

It is important to note that PICON did not fill the conceptual vacuum. It filled the metaphor vacuum. This distinction<sup>30</sup> is important in the case of radio because the public policy discourse had started moving towards “public interest” ever since the realisation that the spectrum is limited and that behaviour of a licensee has an impact on those of the others. In fact, as mentioned earlier, the Secretary of Commerce Herbert Hoover himself talked about the public interest in his speeches at the radio conference. Furthermore, it was not entirely a new metaphor since it also came from the railroads framework, which was already being stretched before the metaphor vacuum occurred. But there was a qualitative difference between the stretching of the railroads framework in the pre and post metaphor vacuum phases. What we call the first order and second order stretching.

In the first-order stretching somewhat forced connections are made between technologies. For instance, radio was linked to railroads via the telegraph and telephone connections. In other words, it would have been difficult to establish a connection between railroads and radio because there is little similarity between them. The telegraph and telephone allowed for the establishment of this connection because they were similar to railroads and also to radio but in different ways. The similarities between railroads and telegraph and telephone networks are rather immediate because they all are composed of nodes and links. On the other hand, the similarities between telegraph and telephone networks and radio rest on the fact they are electronic means of communication. The telegraph and telephone served as intermediaries in linking railroads to radio. This stretched framework functioned as long the new technology was employed in ways that mimicked the old one. The stretching, which was minimal at first, kept widening as new uses of the new technology were found that had no clear analogies in older technologies. Eventually, a breaking point was reached when the old analogs did not work anymore

---

<sup>28</sup> This notion of trusteeship, unlike the commerce clause, allowed for the regulation of licensee’s behaviour because the commission could revoke the license or deny renewal if a licensee was deemed to have violated public trust.

<sup>29</sup> D.R. LE DUC, and T.A. MCCAIN, *o.c.* at p. 396.

<sup>30</sup> As noted, this distinction is important in the case of radio. It does not preclude the fact that a metaphor may also fill in the conceptual vacuum in other contexts.

and we had a metaphor vacuum.

In the post-metaphor vacuum phase the breakthrough came with stretching at a higher level, what we call the second-order stretching. In the pre-metaphor vacuum period, the analog at the technology level was the basis for the transfer of legal concepts. In other words, after an analog was established between railroads and radio via the telegraph and telephone connection, concepts employed for regulating railroads could now be transferred to the radio arena. In the second order stretching, there is stretching at the level of the concepts also. For instance, PICON in the realm of railroads meant something quite different from that in the realm of radio. In the realm of railroads, PICON was based on the logic that since the railroads were granted rights of ways they could be asked to undertake activities in public interests. The same logic was easily transferred to the telegraph and telephone because they also relied on rights of ways. But radio did not use rights of ways. Here the stretching occurred at the level of the rationale for PICON. In the case of radio, the basis of PICON was located in the construction that the licensees are trustees of a scarce public resource, spectrum, and their activities impact the overall culture, especially the socialisation of children. Thus the PICON in the radio context was no longer the same as PICON in its original railroad context. The former was a stretched version of the later.

In the case of radio, the metaphor vacuum was filled by the insertion of a new metaphor of sorts, which brought along with it a legal framework. The other possibility would have been a direct examination of the essential features of the new technology and the development of a brand new framework from scratch based on the first principles of law. We did not see the latter approach in the development of radio regulation. With regard to the Internet, Stephanie Gore asks a provocative question: “Why pick an analogy to begin with? . . . Why shouldn’t courts simply make the effort to understand the technological underpinnings of the Internet and achieve a ‘metaphor-free’ understanding of the technology?”<sup>31</sup> In fact, in the case of the Internet, where also metaphors based on old technologies have dominated the thinking, we at times see the courts recognise the inadequacies of these metaphors and search for new frameworks. For instance, consider the court’s struggle with the applications of libel laws to the Internet Service Providers (ISPs).

In *Stratton Oakmont Inc vs. Prodigy Services Corporation* the plaintiffs sued

---

<sup>31</sup> S. GORE, “A Rose by Any Other Name: Judicial Use of Metaphors for New Technologies”, *University of Illinois Journal of Law, Technology, and Policy*, 2003, Vol. 403, pp. 425-431, at p. 415.

Prodigy for defamatory statements made by an unidentified user on Prodigy's bulletin board service. In its decision the courts held Prodigy to the strict standards normally applied to original publishers of defamatory statements as opposed to treating them as mere distributors, as argued by Prodigy. The court reasoned that Prodigy acted more as an original publisher than as a distributor when it "advertised its practice of actively screening and editing messages posted on its bulletin boards".<sup>32</sup> In sharp contrast to the above judgment, in another court case, *Zeran vs. America Online*, the court rejected analogies with traditional forms of publication such as print, radio and television and refused to impose either a distributor's or a publisher's liability on an online service provider. In this case, the plaintiff Kenneth M. Zeran ("Zeran") who was the victim of a malicious hoax perpetrated via America Online's (AOL) online bulletin board services sued the company for letting these notices remain posted despite his repeated complaints.<sup>33</sup> Countering this accusation, AOL mounted a defence under section 47 U.S.C. § 230, which prohibits the treatment of an ISP as a "publisher" or a "speaker" and therefore the imposition of publisher liability in online defamation cases.<sup>34</sup> In order to go around these section 47 U.S.C. § 230 arguments, Zeran sued AOL as a "distributor" rather than as a publisher.<sup>35</sup> Thus the question before the court in this case was whether to treat AOL as a publisher or a distributor of libellous material. Ruling against the plaintiff, the court said:

[...] "If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement - - from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context [...]. Thus, like strict liability, liability upon notice

---

<sup>32</sup> See *Stratton Oakmont, Inc. vs. Prodigy Services Co.*, 1995, WL 323710 (N.Y. Sup. Ct. 1995).

<sup>33</sup> *Zeran v. America online Inc.*, 129 F.3d at 327, 333 US Court of Appeals 4<sup>th</sup> Cir (1997).

<sup>34</sup> *Zeran v. America online Inc.*, 129 F.3d at 327, 333 US Court of Appeals 4<sup>th</sup> Cir (1997).

<sup>35</sup> This is possible because under common tort law a publisher can be held liable for defamatory statements contained in the works they distribute if they have actual knowledge of the defamatory materials. Given that Zeran had given sufficient notice to AOL about the defamatory statements, he argued that AOL must be held liable as a distributor.

has a chilling effect on the freedom of Internet speech”.<sup>36</sup>

Here we see the courts embrace the metaphors based on old technologies in one case involving libel laws and ISPs and reject the same metaphors in another case. We see similar back and forth movements in other areas of Internet law. Gore (2003) charts such movements in cases involving jurisprudence of jurisdiction. She notes that in *Maritz, Inc. v. Cybergold* the court concluded that “because the internet is an entirely new means of information exchange, analogies to cases involving the use of mail and telephone are less than satisfactory . . .”<sup>37</sup> There is similar divergence of court opinions in cases involving the application of the Single Publication Rule to libel cases on Internet based publications.

Like the radio, much of Internet regulation is based on frameworks from old technologies. The difference is in the cases noted above where the courts rejected parallels with old technologies, something we did not see in the case of radio. Perhaps it was because the radio introduced only one radically new configurational potentiality<sup>38</sup> —point to multipoint

<sup>36</sup> *Zeran v. America online Inc*, 129 F.3d at 327, 333 US Court of Appeals 4<sup>th</sup> Cir (1997), at 333.

<sup>37</sup> *Ibid*, at p.18.

<sup>38</sup> In H. SAWHNEY and S. LEE, “Arenas of Innovation: Understanding New configurational Potentialities of Communication Technologies”, *Media, Culture & Society*, 2005, Vol 27, No.3, pp. 391-414) the authors develop this concept based on Cherry’s notion of “new liberty of action.” While Cherry did not explicitly define the term, he illustrated it with the example of a telephone exchange. According to him, the new liberty of action made possible by the telephone exchange was the “choice of social contacts on demand” (C. CHERRY, “The Telephone System: Creator of Mobility and Social Change”, pp. 112-126 in I. Pool (ed.), *The Social Impact of the Telephone*, Cambridge, MA: The MIT Press, 1977, at p. 114). In other words, for the first time in human history, the telephone exchange offered random access to subscribers dispersed across space. This new technological capability enabled the emergence of new institutional forms that changed how our society is organised. Sawhney and Lee’s reasons for using “new configurational potentialities” instead of “new liberties of action” were twofold. One, the word “liberties” in “liberties of action” generated confusion because of its political overtones. The readers were prompted to see a political dimension in the concept. For example, one reader thought “new liberties” meant empowerment of disenfranchised populations via communication technology. On the contrary, the concept is limited to purely mechanical aspects of how communications channels are configured in a new communications system, point-to-multipoint communication in the case of broadcasting. The new term “new configurational potentialities” avoids this confusion. Two, Cherry’s conceptualisation was limited to features intrinsic to the very nature of a technology. Internet, however, is a multi-modal platform on which myriad configurations, some quite surprising as that of Napster, can be realised. The term “new configurational potentialities” brings forth this broader understanding of the phenomenon.

communication or broadcasting. This new configurational potentiality could be accommodated by a second-order stretch, PICON. What makes the Internet peculiarly different from radio and also other technologies is that it supports not just one radically new configurational potentiality but numerous configuration potentialities, including many that were difficult to imagine a just few years ago. Furthermore, many more radically new configurational potentialities are likely to surprise us in the future. This rapid succession of new developments creates constant strain on the existing frameworks and the courts are often frustrated enough with old metaphors to abandon them. However, they have not yet been able to generate major conceptual breakthroughs that could provide a basis for the development of new frameworks. The establishment of special courts for high-tech cases, as recommended by the Maryland Task Force, would perhaps facilitate direct examination of new technologies. The specially trained judges, with command over technical issues, would be less likely to take refuge in simplifying but inadequate metaphors and make an extra effort to understand the new technology on its own terms.<sup>39</sup>

The suggestion of PICON as a standard was only half the story. Its ready acceptance by the policy makers and the courts is the really critical part. According to Levi (1948), legal process is the application of a “system of rules,” rather than a “known rule,” to diverse facts. Levi notes that, “the rules are discovered in the process of determining similarity or difference. However when attention is directed towards finding of similarities and differences, other peculiarities appear. The problem for the law is: when will it be just to treat different cases as though they were the same?”<sup>40</sup> Therefore a working legal system should be capable of “picking out (intrinsic) similarities and to reason to the justice of applying a common classification”.<sup>41</sup>

The reasoning process using metaphors tends to make similarity a pivotal concept in explanations. However, similarities do not always make analogical reasoning rationally compelling,<sup>42</sup> and legal justifications must be rationally compelling.<sup>43</sup> Therefore in instances where metaphors based on

---

<sup>39</sup> *Ibid.*

<sup>40</sup> E. H. LEVI, *An Introduction to Legal Reasoning*, University of Chicago Press, 1949, quoted in D. HUNTER, “Reason is too Large: Analogy and Precedent in Law”, *Emory Law Journal*, 2001, No 50, pp. 1197-1243, at p.1252.

<sup>41</sup> *Ibid* at p. 1252-1253.

<sup>42</sup> S. BREWER, “Exemplary Reasoning Semantics, Pragmatics and the Rational Force of Legal Argument by Analogy”, *Harvard Law Review*, 1996, Vol 109, No 5, pp. 923-1028.

<sup>43</sup> D. HUNTER, “Reason is too Large: Analogy and Precedent in Law”, *Emory Law Journal*, 2001, No 50, pp. 1197-1243.

older technologies are invoked or when metaphors from dissimilar technologies are stretched and applied to create regulatory frameworks for new technologies or a brand new metaphor is generated, this process is likely to succeed under one important condition. That when rationally compelling arguments can be made and such reasoning relies on seemingly not obvious but intrinsically essential relatedness rather than extrinsically obvious but less essential similarities. In addition such rationally compelling arguments based on metaphors find legitimacy and validity and gain precedence over other arguments when they fit into the existing economic, legal, and regulatory frameworks that have gained legitimacy in the legal system. PICON was readily accepted because it met these conditions, especially those about legitimacy.

Wasserstrom (1961) suggests that when making legal reasoning, we should be careful about dividing reasoning into the “logic of discovery” and the “logic of justification”.<sup>44</sup> While logic of discovery is concerned with insightfulness that can help to find logical connectedness between the two cases, the logic of justification is concerned with whether the reasoning connecting the two is morally justifiable, that is, whether it can have legally compelling justification. In the process of establishing radio regulation systems based on public interest standards, we can say, what the courts did was to make serial attempts to find the logic of justification, whereas what the Congress did was to an attempt to make an insightful discovery, which can be morally justified rather easily in the judicial arena.

## VI. THE IMPACT OF METAPHORS USED EARLY IN THE PROCESS

The radio case alerts us to the strong likelihood that the metaphors used in the early stages of the development of a new technology may not prove to be appropriate over the long run and when the new technology is more developed there may be a need for new metaphors. In the legal context, this could become a sticky problem because precedents set by initial metaphors could make change later on difficult. This problem did not occur in the case of broadcasting where initial metaphors were not an impediment for the adoption of PICON. However, the broadcasting case still demonstrates the stickiness of a metaphor once it is deployed. When Congress considered the 1927 Radio Act, the primary imagery the legislators had for broadcasting was that of airwaves as critical resources

---

<sup>44</sup> R.A. WASSERSTROM, *The Judicial Decision –Towards a Theory of Legal Justification*, 1961, Stanford, California: Stanford University Press, quoted in D. HUNTER, “Reason is too Large: Analogy and Precedent in Law”, *Emory Law Journal*, 2001, No 50, pp. 1197-1243, at p. 1249.

like a “public utility,” such “electricity or water pipe lines”.<sup>45</sup> Accordingly, they focused on the optimal use of a valuable public resource that could be degraded by interference absent appropriate regulation. This conception of broadcasting pushed radio into the public utilities framework, even though the legislators were aware that they were dealing with a form of speech. On the other hand, if the focus had been on speech, they would have had to treat radio as press, with all its first amendment protections, and not a public utility. Therefore, by treating radio as an electrical carrier like telegraph and telephone, they ended up regulating free speech.<sup>46</sup> Later, when the broadcasting aspect of radio became dominant in the 1920s, “the sensitivity of the Supreme Court to the First Amendment” arose.<sup>47</sup> Yet, Congress could go ahead and regulate radio speech without getting stuck in First Amendment litigation because it could point to the special characteristics of radio, especially the fact that it could influence citizens’ children in their own homes. Thus the use of the public utilities framework stymied the subsequent full adoption of the framework traditionally applied to the press.

The impact of the initial metaphor was much stronger in the case of a related technology—cable. It started as rural extensions of TV wherein a local entrepreneur set up an antenna on a mountain top to catch the broadcast signal from a nearby city and then channelled it via coaxial cable to subscribing homes whose direct reception was blocked by the mountain. Since cable was an appendage to broadcasting, at that stage of its development, the policy makers viewed it via the broadcasting framework. Later, after the microwave and satellites links interconnected local cable systems into national networks, cable was transformed into a competing system, as opposed to a mere appendage. Now, in its fully developed form, it seemed too many observers that cable should be regulated as a common carrier and not as a broadcaster.<sup>48</sup> The critical difference would be in the control of the delivery system and control of content. Under the broadcasting regime, a cable operator controlled both the wires and the content that was delivered over them. The common carrier regime would require a separation, i.e. cable operator would have no control over the cable networks (e.g. HBO, CNN, etc) the system carried. The cable operator would lease out bandwidth to other entities that would

---

<sup>45</sup> C. MCLAREN “A brief history of the public interest standard”, 2005, [www.stayfreemagazine.org/ml/readings/public\\_interest.pdf](http://www.stayfreemagazine.org/ml/readings/public_interest.pdf).

<sup>46</sup> I.D.S. POOL, *Technologies of Freedom*. Cambridge, MA, Harvard University Press, 1983.

<sup>47</sup> *Ibid* at p. 232.

<sup>48</sup> *Ibid* at 32; M.O. WIRTH, “Should Cable Television Be Regulated as a Common Carrier?”, Paper presented at the Law and Economics Division of the Law and Society Association Annual Meeting, Denver, Colorado, 1983.

provide the programming. While the common carrier model has its merits and is worth considering, the changeover was no longer practically feasible because by now cable was deeply entrenched within the broadcasting framework. This is not an isolated case because there is a history of new technologies starting off as appendages of the established systems and in unanticipated ways developing into competing systems.<sup>49</sup>

In this paper we offer the above thoughts based on the analysis of a single-case—radio. Quite clearly that it is an insufficient basis for generalisation. But we do hope that we offer a useful starting point. Perhaps the insights offered here will trigger in the readers' minds connections with other cases and thereby get the proverbial snowball rolling. While our specific observations need further testing with other cases, we can quite confidently say that one of the reasons the process proceeds in the way described above is that the metaphors focus our attention on the similarities, a tendency that is reinforced by the legal process that seeks precedents and coherence. Conversely, the peculiarities of the new technology are overlooked. But it is in the peculiarities we get glimpses of the future possibilities opened up by the new technology. In effect, it is the peculiarities that eventually bring about a metaphor vacuum. It therefore behoves us to remain alert to the peculiarities even when we continue to employ metaphors based on old technologies because of the lack of any other device.

---

<sup>49</sup> For other such cases, see H. SAWHNEY, "Public Telephone Network: Stages in Infrastructure Development", *Telecommunications Policy*, 1992, No 16, pp. 538-552; H. SAWHNEY, "Wi-Fi Networks and the Rerun of the Cycle", *Info: The journal of policy, regulation and strategy for telecommunications, information and media*, 2003 Vol 5, No.6, pp. 25-33; H. SAWHNEY, "Wi-Fi Networks and the Reorganization of Wireline-Wireless Relationship", pp. 45-61, in R. LING and P. PEDERSEN (eds.), *Mobile Communications: Re-negotiation of the Social Sphere*, London: Springer-Verlag, 2005.

# **CYBERCRIME, CYBERTERRORISM AND JURISDICTION: AN ANALYSIS OF ARTICLE 22 OF THE COE CONVENTION ON CYBERCRIME**

Armando A. Cottim<sup>\*</sup>

## **I. INTRODUCTION**

Ever since Cain and Abel, crime is a “known known” to human kind. Modern criminal codes have dealt quite well with crime within territorial boundaries and even, sometimes, outside those boundaries, by applying themselves to crimes committed by nationals abroad. Criminal law has then been almost purely domestic, with external threats to the public order of States being dealt with by the military.

Yet, the revolution in information technologies has changed society to a point where advances in programming artificial intelligence software and in the processing capacity of desktop and/or laptop computers are leading society to a time when a cyberbot will be impossible (or at least very difficult) to distinguish from a human person.<sup>1</sup>

And the advent of cyberspace has changed the established criminal law model. Online crime happens without boundaries, as attacks can come from outside the borders of one State, thus scattering crime scenes through two or more countries, sometimes in more than one continent.<sup>2</sup>

Solutions to the problems posed must be addressed by international law, through the adoption of adequate international legal instruments.<sup>3</sup> The

---

<sup>\*</sup> The author has a 5-year law degree achieved at the Lisbon University, Lisbon, Portugal, and was awarded a Master's degree in International Law, by the same University, with a dissertation on Terrorism at Sea in International Law. Being a scuba diving instructor, a musician, a computer programmer and a certified network engineer, his interests float between music, sea and cyberspace. Comments are welcome and can be sent to his email address (armando@cottim.net).

<sup>1</sup> Thus, JOHN J. STANTON, “Terror in Cyberspace. Terrorists Will Exploit and Widen the Gap between Governing Structures and the Public”, in *American Behavioral Scientist*, vol. 45 (2000) p. 1022.

<sup>2</sup> Conveying a similar idea, SUSAN W. BRENNER and JOSEPH J. SCHWERHA IV, “Cybercrime Havens: Challenges and Solutions”, *Business Law Today*, vol. 17 (November/December, 2007), p. 49.

<sup>3</sup> For a thorough study of the relationship between international conventions and international customary law, with special interest in *ius cogens* rules, see EDUARDO CORREIA BAPTISTA, *Ius Cogens em Direito Internacional*, Lisboa, Lex, 1977, pp. 491 *et passim*.

Convention on Cybercrime, opened for signature in Budapest, November 23, 2001 and entered into force in 2004,<sup>4</sup> aimed to meet this challenge – respecting human rights – in the new reality we now call Information Society.

However, although jurisdiction issues were addressed by the Convention on Cybercrime, some weaknesses prevent this Convention from being more effective in making international cooperation the solution for cybercrime. As an additional problem, cyberterrorism also became a hazard the international community has to deal with.

Even if it seems to be a real threat,<sup>5</sup> cyberterrorism is a scare word that plays with the fear of two generally known unknowns – terrorism and technology<sup>6</sup> – and discussions rage the international *fora* dealing with terrorism, crime and cybercrime as to the reality of this threat.

Our initial concern will therefore be the analysis of article 22 of the Convention on Cybercrime, first discussing general jurisdiction theories and then the theories applied by the Convention, together with other issues dealt with in the article. Then, a discussion of several cases dealing with jurisdiction, international cooperation and cybercrime will take us to some reflection on cyberterrorism and the applicability of the jurisdiction rules of the Convention on Cybercrime in cyberterrorism cases.

## II. ARTICLE 22. THE ANALYSIS

---

<sup>4</sup> In accordance with article 36, paragraph 3 of the Convention on Cybercrime, after Albania (signed: November 23, 2001, ratified: June 20, 2002), Croatia (signed: November 23, 2001, ratified: October 17, 2002), Estonia (signed: November 23, 2001, ratified: May 12, 2003), Hungary (signed: November 23, 2001, ratified: December 4, 2003), and Lithuania (signed: 23/6/2003, ratified: March 18, 2004), all members of the Council of Europe, have expressed their consent to be bound by the Convention. For a list of the States that signed and ratified the Convention, see “Convention on Cybercrime. CETS No.: 185”, online at <http://conventions.coe.int>.

<sup>5</sup> For an examination of the use of the Internet by terrorists, extremists and activists, see KATHY CRILLEY, “Information warfare: new battlefields, Terrorists, propaganda and the Internet?” in Alan O’Day (ed.), *Cyberterrorism*, Aldershot, Ashgate Publishing Limited, 2004, pp. 67-74. For a discussion of the widespread use of information technology by terrorist-type organizations in recent years, for propaganda, fundraising, information dissemination and secure communications, see S. M. FURNELL and M. J. WARREN, “Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium?” in Alan O’Day (ed.), *Cyberterrorism*, pp. 113-115.

<sup>6</sup> See AYN EMBAR-SEDDON, “Cyberterrorism: Are We Under Siege?” in Alan O’Day (ed.), *Cyberterrorism*, p. 11.

### 1. *Jurisdiction theories*

No less than five different jurisdiction theories have been applied altogether by courts and governments, all leading to the ascribing of jurisdiction to one court and adversely affecting other courts' jurisdiction.

#### a. Territoriality theory

The theory that jurisdiction is determined by the place where the offence is committed, in whole or in part ("territoriality theory"), derives from the Westphalian<sup>7</sup> model of sovereignty, which is said to include three fundamental principles: □ exclusive control over the nation's territory, □ non-interference, and □ equality between States.<sup>8</sup> Although discussed and opposed,<sup>9</sup> the model seems to have, at least, a general acceptance in what concerns these principles, even if the equality between the States is most of the times only formal.<sup>10</sup>

Given that the State has sovereignty over the territory, it will obviously have jurisdiction over any misconduct which occurs in that territory,<sup>11</sup>

<sup>7</sup> On the Westphalia treaties, see CHRISTOPHER HARDING e C. L. LIM, "The Significance of Westphalia: An Archaeology of the International Legal Order", in Christopher Harding and C. L. Lim (eds), *Renegotiating Westphalia: Essays and Commentary on the European and Conceptual Foundations of Modern International Law*, The Hague / Boston / London, Martinus Nijhoff Publishers, 1999, pp. 1-23.

For a vision on the centrality of the concept of sovereignty derived from Westphalia and the various international relations theories (Marxism excepted), see STEPHEN D. KRASNER, *Sovereignty: Organized Hypocrisy*, New Jersey, Princeton University Press, 1999, pp. 44-46.

<sup>8</sup> Thus, JOAN FITZPATRICK, "Sovereignty, Territoriality, and the Rule of Law", *Hastings International and Comparative Law Review*, vol. 25 (2002), pp. 304,310. SEYOM BROWN, *International Relations in a Changing Global System: Toward a Theory of the World Polity*, Boulder, Colorado, Westview Press, 1992, p. 74, however, refers only two principles: one according to which a State is "unequivocally sovereign within its territorial jurisdiction", and the principle of non-interference.

<sup>9</sup> CHRISTOPHER C. JOYNER and WAYNE P. ROTHBAUM, "Libya and the Aerial Incident at Lockerbie: What Lessons for International Extradition Law?", *Michigan Journal of International Law*, vol. 14 (Winter, 1993), pp. 256, 257, refer that "the Westphalian concept of absolute State sovereignty is undergoing challenge from the community conception espoused by the U.N. Charter", and STÉPHANE BEAULAC, *The Power of Language in the Making of International Law: The Word Sovereignty in Bodin and Vattel and the Myth of Westphalia*, Leiden / Boston, Martinus Nijhoff Publishers, 2004, pp. 71 *et passim*, considers the Westphalian system as a myth, given the centralizing relevance of the sovereignty concept in Bodin and the externalization of authority that Vattel sees in the concept.

<sup>10</sup> Thus, FRANCISCO FERREIRA DE ALMEIDA, *Direito Internacional Público*, 2<sup>a</sup> ed., Coimbra, Coimbra Editora, 2003, p. 15.

<sup>11</sup> Thus, FRANCESCO ANTOLISEI, *Manuale di Diritto Penale. Parte Generale*, 15<sup>a</sup> ed., Milano, Dott. A. Giuffrè Editore, 2000, p. 118.

whether perpetrated or not by one of its nationals.<sup>12</sup>

A complex case of application of the territoriality theory is *Bavaria v. Somm*, tried at the *Amtsgericht* of Munich, Germany, in 1999. As Managing Director of CompuServe Information Services GmbH, Felix Bruno Somm, a citizen from Switzerland, was charged in Germany with being responsible for the access – in Germany – to violent, child, and animal pornographic representations stored on the CompuServe's server placed in the USA.<sup>13</sup> The court considered it had jurisdiction over Mr. Somm because, even though he was Swiss, he lived in Germany.<sup>14</sup>

#### b. Nationality theory

The “nationality theory” is also called “active personality theory” because it deals primarily with the nationality of the person who committed the offence.<sup>15</sup> Being widely recognised that a country has almost unlimited control over its nationals,<sup>16</sup> said country is considered to have the right to exercise jurisdiction over those individuals, wherever they are and whatever they do.<sup>17</sup> Wherever the offence is committed – at home or abroad – the offender probably has better knowledge of the laws of his own State than of the laws of the other State. Also, an act can be

<sup>12</sup> A comparative study of several penal codes in Europe shows that all consecrate the principle of territoriality. Thus, article 6 of the Italian *Codice Penal* states that “Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana.” Following the same path, article 113-2 of the French *Code Pénal* states: “La loi pénale française est applicable aux infractions commises sur le territoire de la République”, section 3 of the German *Strafgesetzbuch* states “[d]as deutsche Strafrecht gilt für Taten, die im Inland begangen werden” and article 4 of the Portuguese *Código Penal* states that “[s]alvo tratado ou convenção internacional em contrário, a lei penal portuguesa é aplicável a factos praticados em território português, seja qual for a nacionalidade do agente.”

<sup>13</sup> *People v. Somm*, Case 8340 Ds 465 Js 173158/95 (Amtsgericht, München, Bavaria, 1999). See, also, THOMAS STADLER, *Der Fall Somm (CompuServe)*, online in <http://www.afs-rechtsanwaelte.de/urteile/artikel06-somm-compuserve1.php>, last visited September 2, 2008.

<sup>14</sup> Mr. Somm was sentenced to an overall term of imprisonment of 2 years (paragraph II of the sentence), even if the following paragraph of the sentence suspended (*ausgesetzt*) its execution on probation.

<sup>15</sup> Thus, CHRISTOPHER L. BLAKESLEY, “Jurisdictional Issues and Conflicts of Jurisdiction”, in M. Cherif Bassiouni (ed.), *Legal Responses to International Terrorism. U.S. Procedural Aspects*, Dordrecht, Martinus Nijhoff Publishers, 1988, p. 139.

<sup>16</sup> Thus, RAY AUGUST, “International Cyber-Jurisdiction: A Comparative Analysis”, *American Business Law Journal*, vol. 39 (Summer, 2002), p. 539.

<sup>17</sup> This statement is not supposed to be understood in an active, dictatorial sense (where the State controls every aspect of the citizens' life), but in a passive, securitarian sense (where the State has the responsibility to protect society against criminal behaviour).

considered legal in the territory where it was committed, whereas it can be considered a crime in the person's homeland.<sup>18</sup>

The case *United States v. Galaxy Sports* seems to be a good example<sup>19</sup> of the application of this theory.<sup>20</sup> World Sports Exchange, together with its President Jay Cohen, was one of the defendants. The company targeted customers in the United States, advertising its business all over America by radio, newspaper, and television. Its advertisements invited clientele to bet with the company either by toll-free telephone or through the Internet.<sup>21</sup> Because the company was Antigua-based, the court was unable to assert jurisdiction over it. Its President, however, was a citizen of the USA and could, therefore, be taken to court. Mr. Cohen was – on August 10, 2000, after a jury trial presided by Judge Thomas P. Griesa – sentenced to a term of twenty-one months' imprisonment.<sup>22</sup> Dealing with the appeal to this sentence, the Second Circuit Court of Appeals affirmed the judgment of the district court without even discussing the assumption of jurisdiction.<sup>23</sup>

<sup>18</sup> The European penal codes mentioned above consider themselves as having jurisdiction with regard to certain actions committed abroad by nationals. Thus, article 9 of the Italian *Codice Penale*, article 113-6 of the French *Code Pénal*, section 5 of the German *Strafgesetzbuch* and article 5 of the Portuguese *Código Penal*.

<sup>19</sup> The sentencing of Robert Matthew Bentley, a citizen of the USA, to 41 months in prison, followed by three years supervised release, together with a restitution of \$65,000, by the federal grand jury in Pensacola, Florida, USA, presided by United States District Judge Richard Smoak, in November 2007, for crimes committed in Europe through the Internet, seems to be another good example of application of the nationality theory for jurisdiction assumption. See UNITED STATES ATTORNEY'S OFFICE, NORTHERN DISTRICT OF FLORIDA, "International Computer 'Hacker' Sentenced to More Than Three Years in Federal Prison", online at <http://www.usdoj.gov/criminal/cybercrime/bentleySent.pdf>, last visited September 2, 2008.

<sup>20</sup> This case was the first U.S. federal action against operators of offshore companies using Web sites to facilitate illegal gambling. The complaint names six companies, one of which is Antigua-based World Sports Exchange. For a short description of the case, see *United States v. Galaxy Sports*, Digestible Law. Perkins Coie's Internet Case Digest, online at <http://www.digestiblelaw.com/gambling/blogQ.aspx?entry=2305&id=16>, last visited September 2, 2008.

<sup>21</sup> For a short description of the company's activity, see *USA v. Cohen*, Second Circuit Court of Appeals, online at <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=2nd&navby=docket&no=001574>, last visited September 2, 2008.

<sup>22</sup> Of which he seems to have served 17 months. See BENNET KELLEY, "Crystalball.Gov: Predicting Cyber Policy in 2008", *Journal of Internet Law*, vol. 11 (March, 2008), p. 21.

<sup>23</sup> See *USA v. Cohen*, Second Circuit Court of Appeals, online, quoted. For a short description of the consequences derived from Mr. Cohen's conviction, see KATHRYN B. CODD, "Betting On The Wrong Horse: The Detrimental Effect of

c. Passive personality theory

While the “nationality theory” deals with the nationality of the offender, assigning jurisdiction to his/her homeland courts, its opposite – the “passive personality theory” – is concerned with the nationality of the victim.<sup>24</sup> The reasons for ascertaining jurisdiction over an offence are similar for both – the almost unlimited control over a country’s nationals – but are now seen from the opposite point of view. Thus, when we follow this theory, the courts of the State to which the victim belongs assume jurisdiction.<sup>25,26</sup>

Good examples of this assumption are the interception of the Egyptian plane that carried the *Achille Lauro* perpetrators by USA planes,<sup>27</sup> and the dispute between the USA and Italy regarding their judgment,<sup>28</sup> together with the several cases presented by the family of Mr. Leon Klinghoffer in North American courts against the Palestinian Liberation Organization, the Lauro company, ABC Tours, Chandris, Inc. (the company that chartered the boat) and the Port of Genoa, Italy.<sup>29</sup>

In the field of cybercriminology, a fine example of jurisdiction assumption by application of the passive personality theory is the sentencing, on July 25, 2003, at the federal courthouse in Hartford, Connecticut, USA, by United States District Judge Alvin W. Thompson, of the Russian citizen Alexey Ivanov, who lived in Chelyabinsk, Russia, for hacking into computers in the United States.<sup>30,31</sup>

---

Noncompliance in the Internet Gambling Dispute on the General Agreement on Trade in Services (GATS)”, *William and Mary Law Review*, vol. 49 (December, 2007), pp. 946 *et passim*.

<sup>24</sup> Thus, CHRISTOPHER L. BLAKESLEY, “Jurisdictional Issues and Conflicts of Jurisdiction”, p. 139.

<sup>25</sup> Thus, JOAN FITZPATRICK, “Sovereignty, Territoriality, and the Rule of Law”, *Hastings International and Comparative Law Review*, vol. 25 (2002), p. 313, note 37.

<sup>26</sup> Article 10 of the Italian *Codice Penale*, article 113-7 of the French *Code Pénal*, Section 7 of the German *Strafgesetzbuch* and article 5 of the Portuguese *Código Penal* apply the respective national criminal law to acts against the nationals of these countries.

<sup>27</sup> For a careful description of the facts, see ANTONIO CASSESE, *Terrorism, Politics and Law: The Achille Lauro Affair*, Cambridge, Polity Press, 1989, pp. 31-43.

<sup>28</sup> For all matters dealing with the interception and subsequent reactions, see GREGORY V. GOODING, “Fighting Terrorism in the 1980’s: The Interception of the Achille Lauro Hijackers”, *Yale Journal of International Law*, vol. 12 (1987), pp. 158-161.

<sup>29</sup> For a description of the civil suits arising out of the *Achille Lauro* incident, see DEAN C. ALEXANDER, “Maritime Terrorism And Legal Responses”, *Transportation Law Journal*, vol. 82 (1991), pp. 467 *et passim*.

<sup>30</sup> *U.S.A. v. Ivanov* (2003), 172 C.C.C. (3d) 551 (Nfld.C.A.). See also U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY, “Russian Man Sentenced

d. Protective theory

The “protective theory” (also called “security principle” and “injured forum theory”) is probably the least used – if ever – of the theories that sanction jurisdiction. Dealing with the national or international interest injured, this theory permits the assignment of jurisdiction to the State that sees its interest – whether national or international – in jeopardy because of an offensive action.<sup>32</sup> In any case, there seems to be a general trend for penal laws to include this theory,<sup>33</sup> sometimes restricting the application to certain crimes, like counterfeiting of money and securities.

e. Universality theory

Finally, the “universality theory” is based on the international character of the offence and, contrary to the other theories, allows every State the claim of jurisdiction over offences, even if those offences have no direct effect on the asserting State,<sup>34</sup> therefore demanding no nexus between the State assuming jurisdiction and the offence itself.

Two requirements are necessary for assuming jurisdiction: □ the State assuming jurisdiction must have the defendant in custody,<sup>35</sup> and □ the

---

for Hacking into Computers in the United States”, online at <http://www.usdoj.gov/criminal/cybercrime/ivanovSent.htm>, last visited September 2, 2008.

<sup>31</sup> Another example is the sentencing – in the federal court of Manhattan, Southern District of New York – of the Kazakhstan citizen Oleg Zezev to 51 months in prison, for extortion and computer hacking charges, due to facts that occurred while he was still living in Almaty, Kazakhstan. See U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY, “Kazakhstan Hacker Sentenced to Four Years Prison for Breaking into Bloomberg Systems and Attempting Extortion”, <http://www.usdoj.gov/criminal/cybercrime/zezevSent.htm>, last visited September 2, 2008.

<sup>32</sup> Thus, CHRISTOPHER L. BLAKESLEY, “Jurisdictional Issues and Conflicts of Jurisdiction”, p. 139.

<sup>33</sup> See *Codice Penale* article 7, *Code Pénal* article 113-10, *Strafgesetzbuch* section 6, and *Código Penal* article 5, number 1, *littera a*) (which specifically deals, *inter alia*, with computer crime).

<sup>34</sup> Thus, CHRISTOPHER L. BLAKESLEY, “Jurisdictional Issues and Conflicts of Jurisdiction”, p. 141.

<sup>35</sup> Questionable means (like abduction) may sometimes have been employed for this. The assumption of jurisdiction over what was (wrongly) considered as piracy led to a questionable action of the USA navy fighters over the commercial plane taking the *Achille Lauro* terrorists from Egypt, after the release of the ship. The Egyptian plane was diverted to a NATO base in Italy. What having the defendant in custody often requires is international cooperation. So, M. CHERIF BASSIOUNI, “Policy Considerations on Inter-State Cooperation in Criminal Matters”, *Pace Yearbook of International Law*, vol. 4 (1992), pp. 126-128. Thus, *v.g.* in the case of Oleg Zezev, Mr. Zezev was called for a meeting in the U.K. and the British police seized

crime must be especially offensive to the international community.<sup>36</sup> Thus, the first crime to be considered for universal jurisdiction was piracy, followed by slave traffic.<sup>37</sup>

After WW II, war crimes, crimes against humanity, certain terrorist acts, hijacking and sabotage of planes, apartheid, torture and other violations of human rights progressively became subject to universal jurisdiction.<sup>38</sup>

## 2. *Jurisdiction Theories applied by the Convention*

---

him after he recognized the facts of his crime in the presence of a disguised British police officer.

<sup>36</sup> Thus, M. CHERIF BASSIOUNI, *Crimes against Humanity in International Criminal Law*, Dordrecht, Martinus Nijhoff Publishers, 1992, pp. 511-513. Mr. Bassiouni also refers that, in the Middle Ages, some cities in Northern Italy would seize and/or persecute certain types of criminals (those they called *banditi*, *vagabundi* and *assassin*) when they were under their jurisdiction, even if the crime was committed elsewhere, therefore applying the principle of universal jurisdiction for specific crime types. M. CHERIF BASSIOUNI, *Crimes against Humanity in International Criminal Law*, p. 513.

<sup>37</sup> Thus, *inter alia*, KENNETH C. RANDALL, "Universal Jurisdiction under International Law", *Texas Law Review*, vol. 66 (March, 1988), p. 788.

<sup>38</sup> Thus, ERIC S. KOBRICK, "The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes", *Columbia Law Review*, vol. 87 (November, 1987), pp. 1523, 1524. This idea is shared by THOMAS H. SPONSLER, "The Universality Principle of Jurisdiction and the Threatened Trials of American Airmen", *Loyola Law Review*, vol. 15 (1969), p. 49, who mentions the Nuremberg and Tokyo trials, after the end of WW II, as the concept's expansion moment.

JAMES D. FRY, "Terrorism as a Crime against Humanity and Genocide: The Backdoor to Universal Jurisdiction", *UCLA Journal of International Law and Foreign Affairs*, vol. 7 (2002), p. 176, refers that the UN General Assembly codified the universality principle, applied in Nuremberg, to war crimes, crimes against humanity and aggression crimes.

The Geneva Conventions of 1949 codified the universality principle in relation to war crimes. The 1948 Genocide Convention did not apply universal jurisdiction to genocide because France, the Soviet Union and the USA opposed, but many courts applied the principle to genocide, considering this should be considered customary international law. Thus, KENNETH C. RANDALL, "Universal Jurisdiction under International Law", p. 789.

On the other hand, JONATHAN I. CHARNEY, "Progress In International Criminal Law?", *American Journal of International Law*, vol. 93 (April, 1999), p. 454, considers that the international illegality of acts such as genocide, crimes against humanity, war crimes and similar will be reinforced as a result of the statute of the International Criminal Court, showing these acts were seen as international crime before that moment.

According to JAMES D. FRY, "Terrorism as a Crime against Humanity and Genocide", p. 176, the principle of universality has been expanded, since de 1940s, to include torture, slave traffic and drug traffic.

An analysis of the several *litterae* of paragraph 1 of article 22 of the 2001 Budapest Convention on Cybercrime (hereafter “the Convention”) shows that the Convention relies exclusively on the territoriality and nationality theories to empower parties to establish jurisdiction.

According to *litterae a* to *c*, any offence established under articles 2 through 11 of the Convention that has occurred in the territory of one Party, in a ship flying its flag or in an aircraft registered under its laws, is to be prosecuted in that State.<sup>39</sup> A Party is, therefore, asked by the Convention to assert territorial jurisdiction if both the person attacking a computer system and the attacked system are located within its territory. The same would be true when the attacked computer system is within a Party’s territory, even if the attacker is in another country.

*Litterae b* and *c* specifically require each Party to establish criminal jurisdiction over offences committed on board of ships flying its flag or aircraft registered under its laws. Already implemented in the laws of many States,<sup>40</sup> this type of jurisdiction assumption is most useful where the ship or aircraft is not located in the Party’s territory (or territorial waters/pace) at the time of the commission of the crime.

Then, according to *littera d*, when one national of one State Party commits one of the Convention-laid down offences in another State, the State of nationality of the offender also has to establish jurisdiction provided, however, the target State criminalises the said offence<sup>41</sup> or the offence was

<sup>39</sup> The fact that a Council of Europe-sponsored Convention follows this path is not surprising, given that, traditionally, the European Court of Human Rights defends an essentially territorial notion of jurisdiction. Thus, *inter alia*, *Öcalan v. Turkey* (Application no. 46221/99), Judgment, 12 March 2003, paragraph 93, and the decision of inadmissibility of *Banković and Others v. 17 countries* (Vlastimir and Borka Banković, Živana Stojanović, Mirjana Stoimenovski, Dragana Joksimović and Dragan Suković against Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and the United Kingdom), Application no. 52207/99, paragraphs 59-61.

<sup>40</sup> Ships are frequently considered to be an extension of the territory of the State. The same applies, *mutatis mutandi*, to aircrafts.

Based on article 91 of the UN Convention on the Law of the Sea, the applicability of the territorial principle to ships should be transparent. Because this was already expressed in 1927, in *The Case of the S.S. “Lotus”*, where the Permanent Court of International Justice assimilated a ship (the Turkish *Boz-Kourt*) to the territory of its Flag state, it would seem to be a very well established principle. Nevertheless, it wasn’t so! In fact, just one year after the *Lotus* decision we find decisions in the opposite direction, held by North American courts, *v.g.* in *Lam Mow v. Nagle*, 24 F.2d 316 (9th Cir., 1928) and *Wong Ock Jee v. Weedon*, 24 F.2d 962 (9th Cir. 1928).

<sup>41</sup> Which means the target State might not be Party to the Convention.

committed outside territorial jurisdiction, of any State, *v.g.* in the High Seas.<sup>42</sup>

Paragraph 4 of the Convention further allows Parties to establish jurisdiction in conformity with their domestic law, which enlarges the base for jurisdiction should a State Party so desire.<sup>43</sup>

### 3. *Non-application clause*

Paragraph 2 of article 22 of the Convention allows Parties to reserve the right to apply – or not – the jurisdiction grounds established in *litterae b* to *d*. States are thus given a great deal of liberty regarding issues related with cybercrime, even if they cannot avoid the obligation of prosecution when the offence is committed in their own territory (paragraph 1, *littera a*).

In practice, and since some offences affect several countries at the same time, this non-application clause could result in no country claiming jurisdiction over one given offence, thinking that surely other countries will have suffered more damage and will, therefore, have priority in prosecuting.<sup>44</sup> Therefore, this paragraph should also include an obligation for affected Parties to consult with each other, so no offence is left without appropriate punishment.

Also, to our understanding, this paragraph seems to be in absolute contradiction with the wording of paragraph 1, which transmits the idea that the adoption, by Parties, of legislative (and other) measures to establish jurisdiction is injunctive.

### 4. *Aut dedere aut judicare*

<sup>42</sup> In this case, it is our understanding that the target of the offence could also be outside territorial jurisdiction.

<sup>43</sup> As an example of this enlargement of jurisdiction, the *Strafgesetzbuch* applies itself to certain acts (*v.g.* assaults against air and sea traffic – *Angriffe auf den Luft- und Seeverkehr* – or trafficking of human beings for sexual exploitation – *Menschenhandel zum Zweck der sexuellen Ausbeutung*) committed abroad regardless of the law of the place of their commission (*unabhängig vom Recht des Tatorts*). See *Strafgesetzbuch*, Section 6.

<sup>44</sup> See SUSAN W. BRENNER and BERT-JAAP KOOPS, “Approaches to Cybercrime Jurisdiction”, *Journal of High Technology Law*, vol. 4 (2004), p. 3. The authors mention the fictitious example of a “script kiddie” who “concocts a new worm and, without really thinking of the potential consequences, launches it on the Internet”, “causing significant damage in numerous countries around the world.”

Paragraph 3 of article 24 establishes the international customary law<sup>45</sup> principle *aut dedere aut judicare*.<sup>46</sup> Should the alleged offender be found in the territory of one Party State (different from the one where the offence was committed), an extradition be required by the offended State, and □ the Party in which territory the alleged offender (requested Party) is constrained by domestic law not to extradite,<sup>47</sup> the requested Party has the duty to prosecute, as well as the legal ability to undertake investigations and proceedings domestically.<sup>48</sup> The underlying idea is the need to ensure that no offence goes unpunished.

The fact that the obligation to prosecute or extradite allows an extension of jurisdiction to the State Party, makes us wonder whether it (the obligation) could be considered “universality by Convention” or, in other

<sup>45</sup> There may be some discussion about this qualification. In spite of that, we believe that the continuous inclusion of the principle in various international Conventions establishes the existing feeling that the principle is customary law. Agreeing, JORDAN J. PAUST, “Above the Law: Unlawful Executive Authorizations Regarding Detainee Treatment, Secret Renditions, Domestic Spying, and Claims to Unchecked Executive Power”, *Utah Law Review*, vol. 2007, issue 2, p. 367, note 51.

<sup>46</sup> Established by various international Conventions, the principle *aut dedere aut judicare* began with Huig de Groot’s formulation *aut dedere aut punire* (extradite or punish), and was adapted because not always the alleged offenders are actually guilty. Thus, ZDZISLAW GALICKI, “The Obligation to Extradite or Prosecute (‘aut dedere aut judicare’) in International Law”, Report of the International Law Commission. Fiftysixth session (3 May-4 June and 5 July-6 August 2004). Annex, p. 312, online at <http://untreaty.un.org/ilc/reports/2004/2004report.htm>, last visited September 2, 2008.

<sup>47</sup> Dealing with principles regarding extradition, article 24, paragraph 5, of the Convention establishes the applicability of the conditions provided by the domestic law of the requested Party.

<sup>48</sup> As an example, paragraph 3 of article 33 of the Portuguese Constitution allows for the extradition of Portuguese citizens only in conditions of reciprocity established by international convention, in cases of terrorism and organized crime, but on the condition the requesting State gives guaranties of a fair and equitable process. Also, according to paragraph 6 of the same article, no one is allowed to be extradited from Portugal when facing the possibility of death or irreversible harm to his/her physical integrity.

Such restrictions would not permit the extradition of a person – of any nationality – from Portugal, let’s say, to China to face cybercrime charges, since China has been known to sentence hackers/cybercriminals to death (thus MARCUS RANUM, *Face-Off: Chinese Cyberattacks: Myth or Menace?* online at [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14\\_gc11321716,00.html](http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gc11321716,00.html), last visited September 2, 2008). One such case happened in Canada, with Chinese hacker Fang Yong being extradited to China to face the death penalty. See “Chinese Hacker Sentenced to Death for Embezzlement”, *People’s Daily*, online at [http://english.people.com.cn/english/200006/13/eng20000613\\_42866.html](http://english.people.com.cn/english/200006/13/eng20000613_42866.html), last visited September 2, 2008.

words, “a limited form of application of the universality principle”. However, this is not the adequate context to discuss the philosophic idea of whether the extension of jurisdiction provided by international conventions can be interpreted this way.

The Party requesting for an extradition should do so pursuant to the requirements and conditions of article 24, paragraphs 1 to 4 of the Convention. The requested Party should comply with paragraph 6 of the said article 24.

#### 5. *Positive jurisdiction conflicts*

Finally, paragraph 5 of the article *sub judice* deals with positive jurisdiction conflicts. This type of conflict may occur because, sometimes, one offence (as described in the Convention) could target victims located in only one State;<sup>49</sup> whereas other times, it could target victims located in several States.<sup>50</sup>

This makes it quite normal that several Parties have jurisdiction over one given offence. To make proceedings efficient, the Convention establishes the possibility that the various Parties that claim jurisdiction over one offence consult with each other in order to determine the proper venue for prosecution.<sup>51</sup>

---

<sup>49</sup> This would be the case of Oleg Zezev, mentioned above, who – from Almaty, Kazakhstan – targeted a company (Bloomberg L.P.) in the USA.

<sup>50</sup> This would be the case of David L. Smith, who was sentenced to 20 months in an US Federal Prison because he was the creator of Melissa, a virulent and widespread computer virus which was found on Friday, March 26, 1999. This virus spread all over the globe within just hours of the initial discovery, apparently spreading faster than any other virus before and disrupted personal computers and computer networks in business and government, in the USA and elsewhere. Melissa was initially distributed in an Internet discussion group called alt.sex. The virus was sent in a file bearing the name “list.doc”, which supposedly contained a list of passwords for websites with sexual contents. As users downloaded the file and opened it in Microsoft Word, a macro inside the document executed and e-mailed the “list.doc” file to the first 50 people listed in the user’s e-mail address book. See, U.S. DEPARTMENT OF JUSTICE. NORTHERN DISTRICT OF OHIO, “Florida Man Indicted for Causing Damage and Transmitting Threat to Former Employer’s Computer System (February 7, 2006)”, online at <http://www.usdoj.gov/criminal/cybercrime/anchetaPlea.htm>, last visited September 2, 2008. (For more information on the Melissa virus, see KATRIN TOCHEVA, MIKKO HYPPONEN and SAMI RAUTIAINEN, “F-Secure Virus Descriptions: Melissa”, online at <http://www.f-secure.com/v-descs/melissa.shtml>, last visited September 2, 2008).

<sup>51</sup> Thus, SUSAN W. BRENNER and BERT-JAAP KOOPS, “Approaches to Cybercrime Jurisdiction”, p. 41.

This would allow for an economy of means because, in some cases, it will be most effective for the States concerned to choose a single venue, whereas in others it may be best for one State to prosecute some of the alleged participants, while one or more other States prosecute another group of alleged offenders. However, since the obligation to consult is not absolute, taking place only “where appropriate”, the effectiveness of this rule seems quite compromised.

### III. JURISDICTION AND CYBERWORLD THREATS

#### 1. *Cybercrime and Jurisdiction*

The fact that – as mentioned above – article 22 of the Convention establishes jurisdiction based on territoriality and nationality grounds seems to actually create more problems than it solves. This is so because of the specific type of offence dealt with in the Convention: one person can send (upload) files whose contents are criminal from one computer in one country to a different computer (the server) in some other country and these files can be seen (downloaded) by viewers all over the world. In this case, where is the offence committed? In the country where the person lives and/or where the files are uploaded, in the country where the server is located or in the several countries where the criminal contents is actually seen? And, if we consider this last situation to be the correct interpretation, what if the viewer lives in a country where those particular contents are not criminal?

##### a. The Yahoo case

A good example of the complexity of the jurisdiction issues that arise in cyberworld is the Yahoo case. Based on the fact that the selling or exhibiting of racist objects, namely Nazi memorabilia, is illegal in France, the *Tribunal de Grande Instance de Paris*, in an *Ordonnance de Référé* of May 22, 2000, ordered Yahoo! Inc and its subsidiary Yahoo France not only to exclude French surfers from sales of Nazi memorabilia (“cesser... toute mise à disposition sur le territoire de la République à partir du site “Yahoo.com””), but also to destroy all the concerned files stored in their server (“détruire toute donnée informatique stockée directement ou indirectement sur son serveur”).<sup>52</sup>

---

<sup>52</sup> For details, see the text of the sentence: TRIBUNAL DE GRANDE INSTANCE DE PARIS, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France*, online at <http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm>, last visited September 2, 2008. “UEJF” stands for *Union des Etudiants Juifs de France*; “Licra” stands for *Ligue Contre le Racisme et l'Antisémitisme*.

In this case, the files<sup>53</sup> were probably uploaded from an unknown source and were stored in a server in the United States. Then, one French court asserted jurisdiction over them because they could be seen in France and its contents was criminalized in France.

But the case does not end here. Dissatisfied with the sentence of the French court, Yahoo decided to file a declaratory judgment action in U.S. District Court in San Francisco, hoping to obtain a ruling that the French court's order could not be enforced against Yahoo in the United States. In its lawsuit, besides discussing computer technical matters regarding the (im)possibility of excluding some users of their site from some of the Web pages (those containing Nazi memorabilia), Yahoo maintained that allowing enforcement of the foreign court's order in the United States would violate the First Amendment. U.S. District Judge Jeremy Fogel of the Northern District of California ascertained jurisdiction over LICRA and UEJF (the French anti-racism associations), agreed with Yahoo regarding the violation of the First Amendment and entered a declaratory judgment in the company's favour.<sup>54</sup>

It was LICRA and UEJF's turn to be dissatisfied, this time with Judge Fogel's ruling, which led them to appeal to the 9<sup>th</sup> Circuit. Eventually, the matter came up for decision before an 11-judge panel of that court and the majority of the judges concluded that the district court had jurisdiction over the defendants (LICRA and UEJF), but the judgment of the district court was reversed.<sup>55</sup>

<sup>53</sup> The files to which the French court wanted no access from French citizens were digital copies of Adolph Hitler's "Mein Kampf" and of the book "Les protocoles des Sages de Sion", the supposed proceedings of a Zionist Congress supposedly held in Basel, Switzerland, in 1897. This book was thought – according to the research of Russian historian Vladimir Burtsev – to have been written by agents of the Okhrana, the secret police of Tsar Nicholas II, who himself seemed to have anti-Semitic ideas (thus, JEAN-MARIE ALLAFORT, "Les Protocoles des Sages de Sion", online at <http://www.nuitdorient.com/n138.htm>, last visited September 2, 2008). Further research from Russian historian Mikhail Lépekhine, done after the opening of Soviet archives to researchers, in 1992, showed that it was, in fact, the Russian forger Mathieu Golovinski who wrote the text while living in Paris. Thus, ÉRIC CONAN, "L'origine des Protocoles des sages de Sion", *L'Express*, 16/11/1999, online at <http://www.phdn.org/antisem/protocoles/origines.html>, last visited September 2, 2008.

<sup>54</sup> *Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme*, N.D.Cal. 2001, Nov. 7, 2001, online at <http://cyber.law.harvard.edu/iso2/readings/yahoo-order.html>, last visited September 2, 2008.

<sup>55</sup> UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, *Yahoo! Inc., a Delaware corporation, v. La Ligue Contre le Racisme et l'Antisemitisme, a French association; L'Union des Etudiants Juifs de France, a French association*, No. 01-17424, D.C. No. CV-00-21275-JF, online at

Could the Convention<sup>56</sup> help solve complex problems like the one presented in this case? It probably could! But would it?

b. Controlling Law and International Cooperation

Immediately after establishing the jurisdiction principles mentioned above, the Convention proceeds to elaborate on international cooperation. Article 23, titled “General principles relating to international cooperation”, creates an obligation for Parties to cooperate with each other in matters related with extradition (article 24), mutual assistance (article 25), spontaneous information (article 26) and some other details.

Good examples of international cooperation are the *Rome Labs* case and the *Tore Tvedt* case.

According to Appendix B of the Staff Statement of the US Senate’s Permanent Subcommittee on Investigations, of June 5, 1996,<sup>57</sup> on March 28, 1994, computer systems administrators at Rome Air Development Center, Griffiss Air Force Base, New York, discovered that their network had been penetrated and compromised by an illegal wiretap computer program called a “Sniffer”, which was covertly installed on computer networks by hackers to illegally collect user logons of authorized users. This program had been covertly installed on one of the systems connected to laboratory's network.

The intruders were found to be a pair of hackers calling themselves “Datastream Cowboy” and “Kuji,” whose identities were unknown. “Datastream Cowboy”, a 16-year old who enjoyed hacking into military networks, was located by an informant, who was able to provide a telephone number and address in the United Kingdom. US Air Force agents established a working relationship with New Scotland Yard agents and they arrested the hacker.<sup>58</sup> At the date of the report, “Datastream

---

<http://caselaw.lp.findlaw.com/data2/circs/9th/0117424p.pdf>, last visited September 2, 2008.

<sup>56</sup> According to the Council of Europe website, the United States of America signed the Convention together with the majority of the Council of Europe members, on November 23, 2001, ratified the Convention on September 29, 2006, and it entered into force in the USA on January 1, 2007. (See online, <http://conventions.coe.int>.)

<sup>57</sup> STAFF STATEMENT. U.S. SENATE. PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, *Security in Cyberspace*, June 5, 1996, Appendix B, online at [http://fas.org/irp/congress/1996\\_hr/s960605b.htm](http://fas.org/irp/congress/1996_hr/s960605b.htm), last visited September 2, 2008.

<sup>58</sup> STAFF STATEMENT. U.S. SENATE. PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, *Security in Cyberspace*, online, quoted, p. 6. See, also, GEORGE MOHAY, ALISON ANDERSON, BYRON COLLIE, OLIVIER DE VEL and RODNEY D.

Cowboy” was pending prosecution in the UK. Three years later, Richard Pryce, *a.k.a.* “Datastream Cowboy”, was fined with £1,200 for the intrusion.<sup>59</sup> Matthew Bevan, *a.k.a.* “Kuji”, was also arrested, waited 18 months for a trial and was acquitted because it was judged not to be in the public interest to pursue the case.<sup>60</sup>

The *Tore Tvedt* case dealt with the posting of racist and anti-Semitic propaganda on the Internet. Tore Tvedt, whose Web page was stored in a North American server, was the founder of the Norwegian far-right group Vigrid (an organization which professes a doctrine that mixes neo-Nazism, racial hatred and religion, claiming to worship Odin and other ancient Norse gods), and was considered responsible for the contents of the Web page – even if it was stored out of Norway’s jurisdiction – and was sentenced by a Norwegian court to seventy-five days in jail with forty-five days suspended, plus two years of probation.<sup>61</sup>

In the *Rome Labs* case, the controlling law was that of the location where the actions in question occurred, the hacker’s location. In the *Tvedt* case, however, the controlling law was that of the country in which the damage was said to have occurred. But both depended on international cooperation to be solved.

However, not all cases deal with good international cooperation. On October 10, 2001, the U.S. Department of Justice announced that Vasiliy Gorshkov, of Chelyabinsk, Russia, had been found guilty on 20 counts of conspiracy, various computer crimes and fraud, which made him face a maximum sentence of five years in prison for each count.<sup>62</sup>

---

MCKEMMISH, *Computer and Intrusion Forensics*, Norwood, MA, Artech House, Inc, 2003, pp. 308, 309, who use this as a case study for security in cyberspace.

<sup>59</sup> See the newspaper news published the day after the sentence was given in DAVID GRAVES, “‘Datastream Cowboy’, 19, fined £1,200 for hacking secret US computer systems”, *Telegraph*, March 22, 1997, online at <http://www.telegraph.co.uk/htmlContent.jhtml?html=/archive/1997/03/22/nhack22.html>, last visited September 2, 2008.

<sup>60</sup> For a short story on Matthew Bevan, see MARK WARD, “History repeats for former hacker”, *BBC News*, online at <http://news.bbc.co.uk/2/hi/technology/4761985.stm>, last visited September 2, 2008.

<sup>61</sup> See the media report with comments at “Norwegian Jailed for Web Racism”, *CNN*, Apr. 23, 2002, online at <http://www.con.com/2002/WORLD/europe/04/23/norway.web/index.html>, last visited September 2, 2008.

<sup>62</sup> Thus, U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY, “Russian Computer Hacker Convicted by Jury”, online at <http://www.usdoj.gov/criminal/cybercrime/gorshkovconvict.htm>, last visited September 2, 2008.

After having discovered that some companies had suffered intrusions from hackers, the FBI created a shell company, called it Invita,<sup>63</sup> and eventually established contact with the hackers and lured them to the U.S. with employment opportunities. After long talks and some online testing, Vasiliy Gorshkov and Alexey Ivanov agreed to a face-to-face meeting in Seattle, where they were asked – by FBI undercover agents – about their hacking skills and assumed responsibility for various hacking incidents and activities. At the conclusion of the Invita meeting, the two men were arrested.<sup>64</sup>

According to court filings,<sup>65</sup> the Department of Justice made several unsuccessful attempts to get Russian authorities to cooperate and seize the contents of the hackers' servers in Russia. The North American agents then accessed two servers in Russia where Gorshkov kept his data and downloaded over 1 Gigabyte of information. Subsequently, they obtained a search warrant to look at the downloaded files and got strong evidence of the men's computer hacking and fraud activities.<sup>66</sup>

This was one case where international cooperation did not function due to a lack of response from one of the sides. However, another case was reported where there was a will to cooperate but the law itself did not allow it.

Tens of millions of computers were affected in May, 2000, when the "Love Bug" virus swept the Internet. The virus was quickly traced back to the Philippines,<sup>67</sup> but then law enforcement officials ran into a problem, as the

---

<sup>63</sup> Describing the company, "High-tech net helped FBI snag alleged hackers", *USA Today*, 02/06/2002, online at <http://www.usatoday.com/tech/news/2001-05-09-fbi-tech-sting.htm>, last visited September 2, 2008, stated: "Invita Security looked like a typical Internet company: it had offices, computers, employees, even a secure computer system. The only thing missing was the customers."

<sup>64</sup> U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY, "Russian Computer Hacker Convicted by Jury", online, quoted.

<sup>65</sup> Reported by ROBERT LEMOS, "FBI "hack" raises global security concerns", *CNET News*, May 1, 2001, online at <http://news.cnet.com/2100-1001-256811.html>, last visited September 2, 2008.

<sup>66</sup> U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY, "Russian Computer Hacker Convicted by Jury", online, quoted.

<sup>67</sup> Supposedly to a Filipino computer student who wrote a thesis on stealing passwords from the Internet. "Love Bug revenge theory", *BBC News*, May 10, 2000, online at <http://news.bbc.co.uk/2/hi/science/nature/743082.stm>, last visited September 2, 2008.

Philippines had no law against hacking.<sup>68</sup> Therefore, despite all the damage done,<sup>69</sup> nobody was ever prosecuted for the “Love Bug” virus. The United States wanted the extradition of the main suspect,<sup>70</sup> and there is an international extradition agreement between the United States and the Philippines. However, the lack of law against hacking in the Philippines made extradition impossible in this case.<sup>71</sup>

In the *Invita* case, the controlling law was that of the country in which the damage was said to have occurred. In the “Love Bug” case, however, the controlling law was that of the location where the actions in question occurred, the hacker’s location. None of the cases depended on international cooperation to be solved. In fact, one was solved by hacking into the servers in another country, whereas the other was not solved at all due to an absence of legislation. Sometimes there is a will, but there is no way!

### c. Jurisdiction Issues

Cybercrime is so broad and can be so complex that becomes very difficult to investigate. And jurisdiction adds to the complexity of investigating a technological matter.<sup>72</sup> This difficulty becomes more evident when dealing with international jurisdiction.

Doctrine considers jurisdiction as defining three levels of authority: □ the

<sup>68</sup> See “Philippine investigators detain man in search for ‘Love Bug’ creator”, CNN, May 8, 2000, online at <http://archives.cnn.com/2000/TECH/computing/05/08/ilove.you.02/index.html>, last visited September 2, 2008.

<sup>69</sup> In the UK alone, British Telecom, Vodafone, Barclays, Scottish Power and Ford UK were among the giant firms affected, together with universities and many companies of variable size. “‘Love Bug’ bites UK”, *BBC News*, May 4, 2000, online at [http://news.bbc.co.uk/2/hi/uk\\_news/736080.stm](http://news.bbc.co.uk/2/hi/uk_news/736080.stm), last visited September 2, 2008.

<sup>70</sup> See, *inter alia*, “Suspected hacker may face extradition requests”, CNN, May 9, 2000, online at <http://transcripts.cnn.com/2000/LAW/05/09/internat.hacking.law/index.html>, last visited September 2, 2008.

<sup>71</sup> Thus, SETH MYDANS, “Philippine Prosecutors Release ‘Love Bug’ Suspect”, *The New York Times*, May 10, 2000, online at <http://partners.nytimes.com/library/tech/00/05/biztech/articles/10virus.html>, last visited September 2, 2008.

<sup>72</sup> Regarding the complexity of investigation, see DAN KOENIG, “Investigation of Cybercrime and Technology-related Crime”, *National Executive Institute Associates*, online at <http://www.neiassociates.org/cybercrime.htm>, last visited September 2, 2008. Peter Stephenson, *Investigating Computer-Related Crime: A Handbook for Corporate Investigators*, Boca Raton, FL, CRC Press, 1999, p. 13, adds that most organizations are not equipped to investigate computer crime.

authority to prescribe (the capacity to establish and prescribe criminal and regulatory sanctions, normally prerogative of a government), □ the authority to judge (the competence to hear disputes, normally prerogative of courts), and □ the authority to enforce (the capacity to compel compliance or to punish noncompliance with its laws, regulations, orders, and judgments, as well as the capacity to investigate suspect behaviours, both normally also prerogative of a government).<sup>73</sup>

The Convention on Cybercrime points the way toward cooperation with respect to criminalizing certain behaviours and pursuing those responsible. It does not, however, resolve the issues of international jurisdiction. The investigation of an international crime will always have to depend on the good will of the third country, or else there is no investigation. However, even if the Convention relies heavily on international cooperation, sometimes – as we have seen – this is not enough to take the investigation to an end. We are, therefore, forced to conclude that the Convention is short on giving States the necessary weapons to fight this type of crime.

As an attempt to remedy this deficiency, we would propose three amendments to the Convention: that the consultations of which we have spoken above were not to take place “where appropriate”, but that they would be established as an obligation;<sup>74</sup> that the Convention itself be effectively considered as an extradition convention between the Parties;<sup>75</sup> and □ that the Convention be amended (or supplemented by additional protocol) to include an internal mechanism that allows police investigators from one Party to perform their work online in another Party, subject only to an informal communication to the authorities in the other Party.<sup>76</sup>

---

<sup>73</sup> Thus, *inter alia*, SUSAN W. BRENNER and BERT-JAAP KOOPS, “Approaches to Cybercrime Jurisdiction”, p. 4. According to IAN BROWNLIE, *Principles of Public International Law*, 5th ed., Oxford, University Press, 2002 (1998), p. 58, law-making capabilities are one of the factors that determine the coexistence between nations.

<sup>74</sup> Should the Convention create an obligation to consult – instead of merely allowing for this consultation, as it does with the current wording – this obligation would have the advantage of permitting the determination of the most appropriate venue for persecution, together with an economy of means that would help the international community in not leaving any crime unpunished.

<sup>75</sup> We are aware that paragraph 3 of article 24, allows a Party to consider the Convention as legal basis for extradition. However, the wording of the Convention is weak. The party “may consider” the Convention as legal basis for extradition, but is allowed to consider the opposite. A stronger wording would, in our view, be recommendable.

<sup>76</sup> The formal request to the other Party’s authorities can be useful when dealing with apprehending people or computers. Nevertheless, in cybercrime, sometimes the investigator has to follow the path of the perpetrator of the offence and may find himself messing with a computer that is physically in a place where he

## 2. *Cyberterrorism and Jurisdiction*

### a. To Be or Not To Be

Cyberterrorism conjures up images of fierce terrorists unleashing catastrophic attacks against computer networks, creating chaos, and paralyzing entire nations. A frightening scenario indeed, but how likely is it to occur? From people in denial to people in distress, opinions come in all flavours.

On the denial corner, strong statements make the day. “There is no such thing as cyberterrorism – no instance of anyone ever having been killed by a terrorist (or anyone else) using a computer” says an editor of one monthly magazine from Washington, DC, USA.<sup>77</sup> Besides arguing that no cyberattack has ever been attempted by terrorists,<sup>78</sup> the main line of reasoning of those in this field is that terrorist organizations usually follow the least resistance path and, therefore, are bound to prefer a cheaper and easier alternative to cyberattacks: physical attacks.<sup>79</sup> Yet, are physical attacks now easier and cheaper?

On the opposite corner, statements come in no weaker form. Carnegie Mellon University computer scientist Roy Maxion is reported to have

---

does not have jurisdiction. A formal request would probably result in losing the evidence. However, an informal communication would allow the investigator to pursue the investigation in time.

In the Invita case, for example, if the North American agents had not entered the Russian servers without permission, there would have been no way to prove that the statements both hackers made at the Seattle interview were true, because it was expected that, as soon as the two suspects’ counterparts in Russia found out about the arrests, they would have destroyed the data.

The data copied from the Russian computers had large databases of credit card information (more than 56,000 credit cards) that were stolen from Internet Service Providers. The two Russian computers also had stolen bank account and other personal financial information of customers of online banking at a couple of North American banks. Should the research have waited for a formal answer ... there would have been no proof and the information would still be usable by others. See U.S. DEPARTMENT OF JUSTICE. UNITED STATES ATTORNEY, “Russian Computer Hacker Convicted by Jury”, online, quoted.

<sup>77</sup> JOSHUA GREEN, “The Myth of Cyberterrorism”, *Washington Monthly*, November 2002, online at <http://www.washingtonmonthly.com/features/2001/0211.green.html>, last visited September 2, 2008.

<sup>78</sup> *Ibidem*.

<sup>79</sup> Referred by SEAN P. GORMAN, *Networks, Security and Complexity: The role of Public Policy in Critical Infrastructure Protection*, Glos, UK, Edward Elgar Publishing Limited, 2005, p. 11.

written, in 2001, to President George W. Bush warning him about the fact that the United States was at grave risk of a cyberattack that could devastate the public mind and the nation's economy more broadly than the September 11 attacks.<sup>80</sup> And the reasoning for this extreme position is based on the findings that al Qaeda operators spent time learning about how to disrupt critical infrastructures through the Internet and had plans to put that knowledge to use.<sup>81</sup> Yet, are things really this bad?

If it is true that they are out there, what is then the measure of danger that cyberterrorists really embody?<sup>82</sup> The reality may have been grasped in July 2002, as the United States Naval War College, working in conjunction with Gartner Research, conducted what they called a "digital Pearl Harbour" simulation. According to the conclusions of this simulation, "a group of hackers couldn't single-handedly bring down the United States' national data infrastructure, but a terrorist team would be able to do significant localized damage to U.S. systems."<sup>83</sup>

The analysts concluded that it would be possible to inflict some serious harm to the US data and physical infrastructure systems, but it would require a syndicate with significant resources, including \$200 million, country-level intelligence and five years of preparation time.<sup>84</sup>

The conclusions then show that a cyberattack on the United States is possible, but would require huge planning and a great amount of financing. Considering the above mentioned *Rome Labs* case, if one 16-year old British

---

<sup>80</sup> See DAN FITZPATRICK, "Cybersecurity expert warns of post-9/11 vulnerability", *Global Security*, September 9, 2003, online at <http://www.globalsecurity.org/org/news/2003/030909-cybero1.htm>, last visited September 2, 2008.

<sup>81</sup> See BARTON GELLMAN, "Cyber-Attacks by Al Qaeda Feared", *Washington Post*, June 27, 2002, page A01, online at <http://www.crime-research.org/library/Barton.htm>, last visited September 2, 2008.

<sup>82</sup> FRED COHEN, "Cyber-Risks and Critical Infrastructures" in Alan O'Day (ed.), *Cyberterrorism*, pp. 1-8, lists several critical infrastructures and mentions nightmare scenarios for each one. He then proceeds to solve every one of those scenarios within a framework ranging from only a few hours to a few days, thus showing that a cyberattack would not create havoc for long. As he mentions the Internet, for instance, he states that there are hundreds of thousands of trained experts that could recreate a functional Internet "in a matter of days" (p. 8). He recognizes, by that, the possibility of one such attack.

<sup>83</sup> MARGARET KANE, "U.S. vulnerable to data sneak attack", *CNET News*, August 13, 2002 11, online at <http://news.cnet.com/2100-1017-949605.html>, last visited September 2, 2008.

<sup>84</sup> *Ibidem*.

boy – with £ 750 worth of equipment<sup>85</sup> – was able to intrude a network connected to the US military, the funding requirement is probably overstated.

Cyberterrorists might not be menacing to kill people directly, as a traditional terrorist attack normally does, but one cyberattack could make life very, very difficult, maybe even destroying or severely damaging the complete economical and social system of one country. We thus conclude that cyberterrorism is definitely a real threat which, unfortunately, is here to stay. And, since the chain of terrorist events after September 11, 2001 shows terrorists to have diversified their targets, we should therefore not overlook the possibility of a cyberattack targeting some other less prepared country than the USA.

If an ounce of prevention is worth a pound of cure, we should learn at least one lesson from the catastrophic terrorism actions perpetrated in New York, Madrid and London: terrorists did not attack from a distance. If a cyberattack is to take place in our countries, it can be masterminded elsewhere, but will probably be executed from within our own networks.

#### b. Hackers, Crackers, Terrorists and Jurisdiction Issues

Hackers tend to be more of a nuisance than a danger. Most of the time, they try unauthorized access to networks for the fun of it, for the challenge, or to put networks to a test.<sup>86</sup> Crackers, however, are criminal hackers that also try unauthorized access to networks, but have malicious intents.<sup>87</sup> Cyberterrorists are people that use cyberterror to achieve political or social change.<sup>88</sup>

---

<sup>85</sup> Thus, DAVID GRAVES, “‘Datastream Cowboy’, 19, fined £1,200 for hacking secret US computer systems”, online, quoted.

<sup>86</sup> ANDREW MICHAEL COLARIK, *Cyber Terrorism. Political and Economic Implications*, Hershey / London / Melbourne / Singapore, Idea Group Publishing, 2006, pp. 37-39, discusses the actions normally attributed to hackers, stating (p. 37) that some have even published their findings, either in academic or nonacademic venues.

<sup>87</sup> *Idem*, pp. 40-42.

<sup>88</sup> *Idem*, p. 46, states that because no legislatively defined meaning of cyberterrorism exists, “the domain is open to debate, dispute, and ultimately, ambiguity.” In this text we are not trying to establish a definitive definition for cyberterrorism, for which reason we employed vague wording, as did DOROTHY E. DENNING, “Cyberterrorism”, Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services, U.S. House of Representatives, May 23, 2000, online at <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>, last visited September 2, 2008, when she wrote: “Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein

Because their motivation and goal is so much different from those of crackers and terrorists, hackers are not likely to either become terrorists or be directly employed by them. For trust reasons, it is not likely that terrorists would hire crackers. But it is not impossible for terrorists to gain hacking skills.<sup>89</sup>

Whatever motivation or goal leads one person (or a group) to hack into a network system, be it hacking, cracking or terrorism, the same jurisdiction problems are present to the investigator and to the judge. Obtaining proof of the action, detaining the suspects and presenting them to a court can only to be achieved with quick reaction and the appropriate international tools. This author believes that international cooperation is the way to achieve this goal; however, he also finds that existing international tools fall short on making international cooperation injunctive.

### 3. *The applicability of Article 22 to cyberterrorism cases*

As a threat, cyberterrorism would probably not justify a convention to deal with it. The explicit inclusion of cyberterrorism in the Convention on Cybercrime by means of an additional protocol would probably suffice. Whatever the choice, it is, however, this author's belief that to fight cyberterrorism there is no need for a definition. The broad acceptance of the 1988 Rome Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation shows there is no need to use "scare words" in order to reach consensus. In fact, it was probably due to the lack of such words that the Rome Convention was so successfully adopted. Thus, given the fear of terrorism in our society, an Additional Protocol to the Convention – either detailing some offences that would be considered cyberterrorism or specifying when the offences established in the Convention should be considered more than just cybercrimes – should be enough.<sup>90</sup>

The effectiveness of this Protocol, as well as of the Convention itself, would however depend on the number of States that ratify them. The fact that the United States of America has ratified the Convention, in

---

when done to intimidate or coerce a government or its people in furtherance of political or social objectives."

<sup>89</sup> Thus, AYN EMBAR-SEDDON, "Cyberterrorism: Are We Under Siege?" p. 15. A. M. COLARIK, *Cyber Terrorism*, p. 51, states "Cyberterrorists exist today. The Osama bin Laden Crew is a group of self-proclaimed cyberjihadists", and proceeds to mention force multiplier tasks that cyberterrorists are supposed to be accomplishing.

<sup>90</sup> This Protocol could also include the amendments referred above (Part II, section A, subsection 3) regarding consultation between the Parties, extradition rules and the inclusion of a mechanism to allow police investigators to perform their search online, subject only to an informal communication to the local authorities.

accordance with its article 36, paragraph 1, *in fine*, is a sign that major non-Council of Europe Member States will be willing to cooperate with Member States in the fight against cybercrime and, obviously, against cyberterrorism. Yet, although the Convention entered into force in July 1, 2004, key Member States of the COE – *v.g.* Germany, Russia, United Kingdom, Spain, Austria, as well as the author's own country, Portugal – have not (as of September 1, 2008) ratified the Convention, a situation that can spawn great concern.

#### IV. CONCLUDING REMARKS

Jurisdiction, or the lack of it, seems to be the most problematic issue in the fight against cybercrime and cyberterrorism. The fact that cyberattacks can come from anywhere in the world makes investigation, producing evidence and taking the offenders to court an immense task that can only be achieved through international cooperation.

The Convention on Cybercrime was designed to help accomplish the goal of reducing and/or tearing down the difficulties of the fight against cybercrime. Still, it shows itself to be insufficient because international collaboration is not injunctive and there are no rules to unload the burden of formality from the work of police specialists in charge of investigating international cybercrime/cyberterrorism cases.

Furthermore, the fact that key Member States of the Council of Europe are taking their time to ratify the Convention also leaves a bitter notion of lack of interest in cybercrime, one type of crime that is becoming increasingly important for companies all over the world. Let's hope our countries don't wake up too late. It is easy to be wise after the event!

As a final note, we would like to say that, given the path towards catastrophism and indiscriminate attack on human lives taken by modern day terrorism, we would consider possible and positive the inclusion of terrorism in the list of international crimes against humanity – in accordance with *littera k* of number 1 of article 7 of the Rome Statute of the International Criminal Court (ICC) – which would entitle States to have universal jurisdiction to apprehend terrorist agents, although jurisdiction to prosecute would be given to the International Criminal Court.

Thus, since, in the case of international conventions, the authority to prescribe still rests with the government of the State Party – because no State is forced into being a Party to a Convention and all States still have the right to sign (or not) and ratify (or not) any given Convention – the governments of the Member States concerned would only forfeit the

authority to judge to the International Criminal Court. All States would keep the authority to prescribe, both domestically and by means of ratification of conventions, and the authority to enforce, should the International Criminal Court convict the agents.

# **CHILD PROTECTION ONLINE: UNEASY STEPS TOWARDS A BALANCE BETWEEN RISKS AND FREEDOMS**

Federica Casarosa<sup>\*</sup>

## **I. THE WEB GROWS “YOUNGER”**

Nowadays the Internet has become a digital universe accessible within the comfort of one's household. Although it was originally created as a means of communication in the scientific community,<sup>1</sup> it has developed into an extraordinary diffused medium used in homes, offices, schools, businesses and public administrations.

Moreover, Internet penetration and use of new technologies is still growing considerably in the European Community. This situation is not only due to qualitative improvements of technologies, but it is also related to the wider access of youngsters to this medium. As a matter of fact, a recent survey of the Eurobarometer provided evidence about the rising share of Internet usage by children up to 16 years, (for instance, in European countries, the percentage of children using Internet has reached the rate of 51% in 2006, while the first contact with new technologies lowers down to 6-8 years old).<sup>2</sup>

As a matter of fact, children and young people are more and more often the first to take up and use new technologies; yet, they are not always aware of both risks and ways of dealing with them, or, whether they are, they are not always mature enough to evaluate the situations that they encounter and the possible consequences their decisions can have.

At the end of the day, new technologies can improve the quality of life for children and young people, providing them better access to knowledge and widest possibilities to socialise and experiment social skills. But, at the same time, such resources could also lead minors to decide on issues that normally they would not have to decide in real life, in particular concerning their own safety.

---

<sup>\*</sup> Research Fellow, Università di Trento (I)

<sup>1</sup> In reality, the first usage was a default communication network among military service nodes in the whole United States, and then the technical structure was devoted to the connection of Universities.

<sup>2</sup> See the OPTEM REPORT, *Safer Internet for Children – Qualitative Study*, May 2007, requested by the DG Information society and Media, where the rate of less than 6 years-old children using the Internet is 9%, and from 6-7 years jumps up to 34% (growing further as age increases).

Recent studies shows that new risk situations arise for children with the further diffusion of new Internet enabled end-user devices, like “3G” mobile phones and new practices such as social networking<sup>3</sup> (where chatting includes also the possibility to use web-cams), Internet blogging<sup>4</sup> or file sharing.<sup>5</sup> Moreover, possible future technological developments and user options can increase this risky environment, also through convergent services and new modes of communication. This increase in connectivity by children will see a corresponding increase in benefits for them, but also in risks of “collateral damage”. Dangers, especially for children, and abuse of the technologies continue to exist and new threats and abuses are emerging.

This paper will address, in part II, European interventions concerning children protection online distinguishing the main objectives of such interventions and the preferred tools to achieve an acceptable level of protection; part III will be then devoted to the identification of potential risks for children online, while part IV will analyse the advantages and disadvantages of the tools proposed by European institutions. In part V, a case study will be proposed, concerning social networking, in order to verify if technical and legal tools can be effective in practice. Finally, preliminary conclusions will be presented.

## II. EU INTERVENTION

The European Union has been a forerunner in tackling children protection

---

<sup>3</sup> A social network service focuses on building online communities of people who share interests and activities, or who are interested in exploring the interests and activities of others. Most social network services are web based and provide a variety of ways for users to interact, such as e-mail and instant messaging services. The main types of social networking services are those which contain directories of some categories (such as former classmates), means to connect with friends (usually with self-description pages), and recommender systems linked to trust.

<sup>4</sup> A blog (a contraction of the term “Web log”) is a Web site, usually maintained by an individual, with regular entries of commentary, descriptions of events, or other material such as graphics or video. Many blogs provide commentary or news on a particular subject; others function as more personal online diaries. A typical blog combines text, images, and links to other blogs, Web pages, and other media related to its topic. Most blogs are primarily textual, although some focus on art, photographs, sketches, videos, music, audio, which are part of a wider network of social media.

<sup>5</sup> File sharing refers to the providing and receiving of digital files over a network, usually following the peer-to-peer (P2P) model, where the files are stored on and served by personal computers of the users. Most people who engage in file sharing on the Internet both provide (upload) files and receive files (download).

issues: the first steps date back to 1996, when the Green Paper on the protection of minors and human dignity in informational and audiovisual services was published.<sup>6</sup> It presented a three-part analysis about the existing background concerning the fight against the dissemination of content offensive to human dignity, and the protection of minors against exposure to content that is harmful to their development. Firstly, it described the evolution of audiovisual and information services from a centralised mass media model to a decentralised and individual communication model. Secondly, it analyses the current legislation and policies at national, European and international level, and finally, it pushed forward some guidelines to provide a more flexible regulatory framework capable to face the characteristics of new services.

In particular, the Green Paper stressed the fact that: *“The full potential of such developments [i.e. audiovisual and informational services] will depend on society as a whole striking the right balance between freedom of speech and public interest considerations, between policies designed to foster the emergence of new services and the need to ensure that the opportunities they create are not abused by the few at the expense of the many”*.

At the same time, the Commission published a Communication on Illegal and Harmful Content on the Internet,<sup>7</sup> which provided short-term measures required to deal with specific Internet related issues that go beyond the field of protection of minors and human dignity. In particular, it defined the difference between illegal and harmful content. The former may be banned for everyone, regardless of the age of the potential audience or the medium used (e.g. child pornography, extreme gratuitous violence and incitement to racial or other hatred, discrimination, and violence). The latter, on the contrary, can be defined as *“content that is legal, but liable to harm minors by impairing their physical and mental development”*,<sup>8</sup> thus, access to it can be allowed only for adults.<sup>9</sup> The key difference between harmful and illegal content is that the former is subject to personal choice, *“based on one’s beliefs, preferences and social and cultural traditions”*,<sup>10</sup> while the latter is a matter of state choice. This distinction is essential not to confuse the different objectives and different problems

---

<sup>6</sup> 16 October 1996, COM (96) 483.

<sup>7</sup> Communication on illegal and harmful content on the Internet, COM(96) 487

<sup>8</sup> Ibidem, par. 17.

<sup>9</sup> Later, the Safer Internet Action Plan added to this taxonomy also unwanted material, like spam or undesired commercial communications. See *infra* in the Safer Internet Action Plan Plus.

<sup>10</sup> J.P. MIFSUD BONNICI and C.N.J., DE VEY MESTDAGH, ‘Right vision, wrong expectations: the European Union and self-regulation of harmful Internet content’, *Information & Communications Technology Law*, Vol. 14, No. 2, 2005, 142.

which each of them raises, and consequently the different solutions chosen in each case. With regard to illegal content, the state decides which content should be considered illegal and what consequences should be linked to this classification (for instance, prohibition of publication and distribution).<sup>11</sup> When tackling with harmful content, on the other hand, it is argued that the state should create an environment that enables citizens to decide for themselves (and eventually for their children) which content they consider suitable and worth accessing. Moreover, the recommendation underlined that, in this case, a balance must be struck between possible harm to minors and the preservation of the freedom of expression.

These two measures set the ground for the following community interventions that led to the current regulatory framework.

The following phase was the adoption of the Council Recommendation 98/560/EC, of 24<sup>th</sup> September 1998,<sup>12</sup> on the development of competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity, which defined the guidelines for the national legislation on this issue.<sup>13</sup> In particular, it fostered a European and international cooperation, and it encouraged a more systematic coordination between government, industries, the other parties concerned in each Member State in order to enable minors to make responsible use of online audiovisual and information services, by improving the level of awareness among parents,

---

<sup>11</sup> As far as *illegal content* is concerned, the point of departure is that what is illegal offline is illegal online. It should be ensured that the law is adapted so that it reflects the values of society and deals with new social phenomena. A further area of concern is the degree to which national law can be applied to activities taking place on a global network, whether under application of national rules of conflict of law or in practice. This is difficult if acts are punishable in one country and not punishable in another.

<sup>12</sup> Council Recommendation 98/560/EC of 24 September 1998, OJ L 270, 7.10.1998, p. 48.

<sup>13</sup> It is useful to note that the legal base of this recommendation was Article 130 of the EC Treaty, (actual Article 157 ECT), which requires the Community and the Member States to ensure that the conditions necessary for the competitiveness of the Community's industry exist, with action aimed, *inter alia*, at fostering better exploitation of the industrial potential of policies of innovation, research and technological development. Differently, the following interventions are based on Article 153(2) ECT, on protection of the consumer, since they are focus on the end-user – particularly parents, educators and children – and are intended to promote their safety when using the Internet and new online technologies.

educators, and teachers about the potential of the new services.<sup>14</sup>

In 1999, the aforementioned Recommendation was integrated by the first active intervention in the field: the implementation of a 'Safer Internet Action Plan' (IAP), which identified areas for concrete measures where Community resources should be focused on.<sup>15</sup> The Action Plan defined four specific objectives: the creation of a safer environment (through a network of hot-lines, and the adoption of codes of conduct), the development of a filtering and rating system, the encouragement of awareness-raising actions, and other supporting action (like the assessment of legal implications and the coordination with other similar international initiatives).

After the positive outcome of this four-year plan,<sup>16</sup> the Commission proposed a new mandate for an extended Safer Internet Action Plan (so called IAP-Plus),<sup>17</sup> and the Council of Ministers has recently adopted the new Safer Internet Programme proposed by the Commission for 2009-2013.<sup>18</sup> This new Action plan is designed "to be able to take into account

---

<sup>14</sup> The recommendation was updated in 2006, (*Recommendation on the protection of minors and human dignity and on the right of reply*, 2006/952/EC) following the same objectives. One important difference, however, is the limited role given to self-regulation as a tool to provide effective protection, downgrading it to an additional measure that, alone, cannot be sufficient to protect minors from messages with harmful content; whereas, in the previous recommendation, the role of self-regulation was much more emphasised, also providing the principles on which a self-regulatory intervention should be based (involvement of all interested parties, definition of the objectives in the codes of conduct, cooperation at community level, and regular evaluation of the measures taken).

<sup>15</sup> European Parliament and European Council, *Decision 276/1999/EC of 25 January 1999 adopting a Multi-annual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors* (OJ L 33, 6.2.1999, p.1) as amended by Decision 1151/2003/EC of the European Parliament and of the Council of 16 June 2003 (OJ L 162, 1.7.2003, p. 1).

<sup>16</sup> See the European Commission, *Communication to the Council, the European parliament, the European economic and social committee and the Committee of the regions concerning the evaluation of the multi-annual community action plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors*, COM(2003) 653 final.

<sup>17</sup> European Parliament and European Council, *Decision 854/2005/EC of 11 May 2005 establishing a multi-annual community programme on promoting safer use of the internet and new online technologies*, (OJ L 149 11.6.2005, p.1).

<sup>18</sup> European Parliament and European Council, *Proposal for a Decision establishing a multi-annual Community programme on protecting children using the Internet and communicating technologies*, COM(2008) 106 final, 27 February 2008, approved by the Council of Ministers on the 9<sup>th</sup> December 2008, available at

*currently unknown future developments in the online environment as the resulting threats will become increasingly important in the years ahead*". The actions include again the promotion of a safer online environment and the public-awareness raising action, but these are framed to encompass a better 'user-empowerment' not only for parents and carers but also for children and young people, and to stimulate stakeholders to take responsibility, cooperate and exchange experiences and best practices at European and international level. Moreover, the Action plan acknowledges the need to create and build up an adequate knowledge base for addressing both existing and emerging uses, risks and consequences, and mapping both quantitative and qualitative aspects in this context; thus, it propose the setting of a coordinated investigation activity that will be used immediately in the implementation of the programme, as well as into designing adequate actions for ensuring online safety for all users.

All the European interventions in this field have a non-binding character, moreover, they all support the development and the implementation of technical tools<sup>19</sup> and, among legal tools, they recommends mainly self-regulation as the best regulatory solution. This option is not only due to the fact that technical tools and self-regulation can have a higher level of flexibility and can be better fit with the needs of an ever-changing environment, but also to the general argument – clearly stated in IAPs decisions – that "[r]eaching international agreement on legally binding rules is desirable but will be a challenge to achieve and, even then, will not be achieved rapidly. Even if such agreement is reached, it will not be enough in itself to ensure implementation of the rules or to ensure protection of those at risk".<sup>20</sup>

### III. THE EXISTING RISKS FOR CHILDREN

Having described the current legal framework at European level, it is now necessary to provide the existing threats that children face during online surfing. This will help the analysis concerning the effectiveness of the technical and self-regulatory tools proposed by European and national actors.

#### I. *Child abuse material*

In this category are included the cases in which children are harmed

---

<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1899&format=HTML&aged=0&language=EN&guiLanguage=en>

<sup>19</sup> See *infra* par. IV.

<sup>20</sup> Proposal for a Decision establishing a multi-annual Community programme on protecting children using the Internet and communicating technologies, *cit.*, whereas (5). Previously also in Decision 854/2005/EC, whereas (6), *cit.*

directly, as victims of sexual abuse documented through photographs, films or audio files and then transmitted online. In general child pornography refers to material depicting children being in a state of undress, engaged in erotic poses or sexual activity. Child sexual abuse occurs in the production of child pornography when sexual acts are photographed, and the effects of the abuse on the child (and continuing into maturity) are compounded by the wide distribution and lasting availability of the photographs of the abuse. For practical reasons, legal definitions of child pornography generally refer to a wider age range, including any pornography involving a minor, according to jurisdiction.

## 2. *Child grooming*

In this category are included the cases in which children are contacted by people who will befriend them in order to commit sexual abuse. Thus, the act of grooming a child sexually may include activities that are legal in and of themselves, but later lead to sexual contact. Typically, this is done to gain the child's trust as well as the trust of those responsible for the child's well-being. Sexual grooming of children also occurs on the Internet. Some abusers will pose as children online and make arrangements to meet with them in person.

## 3. *Cyber-bullying*

In this category are included the cases in which children are victims of bullying in the online environment.<sup>21</sup> Cyber-bullying involves the use of information and communication technologies to support deliberate, repeated, and hostile behaviour by an individual or group that is intended to harm others. This can occur not only through text message but also through videos being uploaded on open video-sharing website (e.g. YouTube),<sup>22</sup> having an even more distressing effect, because the bullying in online environment has a potentially enormous audience, extending the humiliation and embarrassment of the victim.<sup>23</sup>

---

<sup>21</sup> Despite this definition, the phenomenon is not limited to children, though is more commonly referred to as cyberstalking or cyber-harassment when perpetrated by adults toward adults. Cyber-bullying can be as simple as continuing to send e-mail to someone who has said they want no further contact with the sender, but it may also include threats, sexual remarks, pejorative labels (i.e., hate speech), ganging up on victims by making them the subject of ridicule in forums, and posting false statements gossip as fact aimed at humiliation.

<sup>22</sup> Cyber-bullies may disclose victims' personal data (e.g. real name, address, or workplace/schools) at websites or forums, or may pose as the identity of a victim for the purpose of publishing material in their name that defames or ridicules them.

<sup>23</sup> Home Office Task Force on Child Protection on the Internet, *Good Practice Guidance for the Providers of Social Networking and User Interactive Services* 2008,

#### 4. *Unlawful privacy invasion*

In this category are included the cases in which children are asked to disclose personal information that can be used to profile them and send them commercial advertising. In this case, the risk is not merely the collection of personal information from children without their, or their parent's, consent.<sup>24</sup> Rather, in wider perspective, the risk involves "*the opening up of the child's private world to the eye of the marketer, who not only watches the child but reconstructs the child's environment in order to manipulate the child's sense of self and security*".<sup>25</sup> The possibility to obtain details of children's online behaviour can provide a continuous feedback to marketers, who not only can select easily which product sale to individual children, but also can fine tune with child's online social environment to make the child more vulnerable to advertising messages. This kind of marketing raises serious questions as it constitutes an invasion of privacy because enterprises penetrate child's private space and extracts data for instrumental purposes by manipulating also their online environment.

### IV. TECHNICAL AND LEGAL TOOLS PROPOSED BY THE EU

Now, we turn to the technical and legal tools proposed and implemented through the Safer Internet Action Plans, in order to analyse which are their advantages and disadvantages.

*Hotline networks:* hotlines are contact points where end-users can report illegal content on the Internet. All hotlines are intended to work together with police, law enforcement and awareness nodes as well as with Internet Service Providers, industry organisations and other institutions. Under the Safer Internet Action Plan a widespread system of hotlines all over Europe had been developed, coordinated by INHOPE, the International Association of Internet Hotlines.<sup>26</sup>

---

available at <http://police.homeoffice.gov.uk/publications/operational-policing/social-networking-guidance?view=Binary>, p. 17.

<sup>24</sup> Privacy concerns exist wherever personally identifiable information is collected and stored - in digital form or otherwise. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, such as: healthcare records, criminal justice investigations and proceedings, financial institutions and transactions, biological traits, such as genetic material, residence and geographic records, ethnicity. The challenge in data privacy is to share data while protecting personally identifiable information.

<sup>25</sup> V. STEEVES, "It's Not Child's Play: The Online Invasion of Children's Privacy", *University of Ottawa law & technology journal*, 2006, 169-188, p. 186.

<sup>26</sup> See the website: [www.inhope.org](http://www.inhope.org).

|               |                                                                                                                                                                                                                                                                                                               |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advantages    | Better knowledge concerning the rate of illegal content available online.<br>Cooperation though-out Europe in order to identify child-porn rings.<br>Centralised reaction in case of multiple jurisdiction issues                                                                                             |
| Disadvantages | Difficult cooperation between hotlines and other stakeholders, in particular with police and law enforcement, (effectiveness of procedures in still low).<br>Lack of feedback from law enforcement authorities in order to improve the process.<br>Low awareness of the existence of hotlines from end-users. |

*Rating and filtering schemes:* a rating system is a technological device that can help the user to identify in advance which are the contents of the website to be visited, usually the rating system describes the content in accordance with a generally recognised scheme (for instance, where items such as sex or violence are rated on a scale) and then filtering systems can empower the user to select the content he/she wishes to receive. Ratings may be attached by the content provider or provided by a third-party rating service. There are a number of possible filtering and rating systems.<sup>27</sup>

|               |                                                                                                                                                                                                                     |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advantages    | possibility to filter in advance the content to be viewed by user<br>flexible tool (e.g. to be adapted to different aged children)                                                                                  |
| Disadvantages | Low level of sophistication.<br>Difficult to achieve a critical mass need to provide accountable results.<br>Difficult to identify the appropriate labels in order to avoid that innocuous content will be blocked. |

*Age verification tools:* obviously this kind of tool aims at ascertaining in advance the age of online user so as to keep older people away from youngsters, or vice-versa, keep young people away from website designed for adults. To accomplish either of those objectives, such tools must be able to effectively verify everyone's age by consulting reliable records about

---

<sup>27</sup> See for instance the Platform for Internet Content Selection (PICS), which is a specification created by World Wide Web Consortium that uses metadata to label webpages to help parents and teachers control what children and students can access on the Internet. See more deeply at: <http://www.w3.org/PICS/>

those looking to create an account on a social networking site. However, if the age verification is posed on adult's identity the proofs can be obtained from many sources,<sup>28</sup> while in case of children proving their age becomes more complicated, as only few can provide a similar set of proofs. Moreover, age verification can provide only a limited security effect, i.e. distinguish who can access or not to a specific website on the basis of its age; whereas no control at all is to be done on the records of the person accepted (e.g. existence of previous sex related crimes, etc.), thus, providing a false perception of security either to parents and to children.<sup>29</sup>

|               |                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advantages    | limitation of access to adults in children websites and vice-versa                                                                                                      |
| Disadvantages | difficult to achieve the perfect age verification<br>false sense of security for both parents and children<br>difficult coordination with freedom of speech and privacy |

#### *Codes of conduct:*

As said before, the European Commission promotes the use of self-regulation to provide a The Commission does not provide a specific model of self-regulation, rather it accepts the existence of multiple choices,<sup>30</sup> including codes of conduct; however, in any model drawn up by the relevant actors, the principles that it should respect are those of effectiveness, fairness, and transparency.<sup>31</sup> Furthermore, in case of codes of conduct, they should provide credible mechanisms for monitoring compliance, taking complaints and sanctions for non-compliance, together with means of making the public aware of their existence.<sup>32</sup>

<sup>28</sup> See that when government officials or even business seek to verify someone's identify or age, they can rely on birth certificates, Social Security numbers, driver's licenses, military records, home mortgages, car loans, other credit records, or credit cards.

<sup>29</sup> A. THIERER, "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions", *Progress & Freedom Foundation Progress on Point* 14.6, 2007, available at [www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf](http://www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf)

<sup>30</sup> See, J-F. LEROUGE, "Internet Effective Rules: the Role of Self-regulation", in *The Edi Law Review*, 2001, 199 ff., where the Author lists the different forms of regulation: the "simple" unilateral declaration of will, the adoption of codes of conduct, the contract, the certification or labelling methods, the common practice or the emergence of a "lex electronica".

<sup>31</sup> See the guidelines already defined in the Recommendation 98/560/EC, cit., where the principles on which a self-regulatory intervention should be based were spelled out.

<sup>32</sup> According to a widely accepted definition, self-regulation norms are legal rules voluntarily created by a group of persons or their representatives from a particular sector of activities, accessible to them and therefore susceptible to be known by

|               |                                                                                                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Advantages    | quick reaction to public concerns<br>flexible tool<br>expertise of industry players                                                                                                                                   |
| Disadvantages | Limited level of enforceability<br>Risks of 'private censorship', as commercial organisations can decide what content can be considered harmful<br>Low awareness of the existence of codes of conduct from end-users. |

## V. CASE STUDY: SOCIAL NETWORKING

We now turn to a case study, taking an example easily available on the Internet: social networking, so as to verify the adaptability of the previously listed tools, and eventually provide the better synergy among them.

One of the most evident developments of Internet communication is its increasingly dynamic and interactive nature. Social networking is one of the new phenomena that bloomed in this evolved environment.<sup>33</sup> In social networks, users, once registered, can make public their personal data in order to establish a set of contacts with others who went to the same schools or universities (such as in *facebook.com*),<sup>34</sup> or who work in the same sector or firm (such as in *linkedin.com*),<sup>35</sup> or even in order to make self-promotion (such as in *myspace.com*).<sup>36</sup> In all these cases, users make available personal information, including sensitive data, to the entire circle of registered users. This behaviour can simplify the collection and the elaboration of users' profiles, giving leeway also to secondary use by third

---

them and subject to sanctions in case of non-compliance, see J-F. LEROUGE, "Internet Effective Rules", cit., 197.

<sup>33</sup> These services are considered to be part of a paradigm shift in the evolution of the Internet, which is now frequently referred to as Web 2.0. Web 2.0 represents a fundamental shift away from this model, towards a more dynamic and interactive Internet where the creation of content is decentralised and more controlled by individuals or communities of users.

<sup>34</sup> See <http://www.facebook.com>. On this issue see I. BROWN, L. EDWARDS e C. MARSDEN, "Stalking 2.0: privacy protection in a leading social networking site", paper presented at the conference "GiKii returns", London University College, 19 September 2007, available at <http://www.law.ed.ac.uk/ahrc/gikii/docs2/edwards.pdf>, and more recently L. EDWARDS and I. BROWN, "Data control and social networking: irreconcilable ideas?", available at <http://ssrn.com/abstract=1148732>.

<sup>35</sup> See <http://www.linkedin.com>

<sup>36</sup> See <http://www.myspace.com>

parties, who can take advantage of such information in different ways.<sup>37</sup> Potential risks to children and young people using social networking services can include but are not limited to:

- bullying by peers and ‘friends’;
- exposure to inappropriate and/or harmful content;
- posting illegal or inappropriate content;
- posting personal information that can identify and locate a child offline;
- download viruses and *malware*;
- sexual grooming, exploitation and abuse through contact with strangers;
- exposure to information about self-harm techniques or encouraging anorexia and suicide;
- identity theft;<sup>38</sup>
- race hatred; etc.<sup>39</sup>

How can these risks be faced and overcome through the aforementioned tools ?

Technical tools can help limiting the diffusion of children personal data. For instance, an ‘age locking’ can set profiles of users under eighteen automatically private, thus protect them from being viewed by adult users that they don’t already know in the physical world.<sup>40</sup> This can be a useful

---

<sup>37</sup> G. MACCABONI, “La profilazione dell’utente telematico fra tecniche pubblicitarie on-line e tutela della privacy”, *Riv. Dir. Inf. e Informatica*, 2001, 425; C. D’AGATA, ““Self” e “strict” regulation: il trattamento dei dati personali nell’approccio “pluridisciplinare” di tutela introdotto dal codice della privacy”, *Riv. Dir. Inf. e Informatica*, 2004, 883; L. EDWARDS e G. HOWELLS, “Anonymity, consumers and the Internet: where everyone knows you’re a dog” in C. NICCOL, J.E.J. PRINS, M.J.M. VAN DELLEN (eds.), *Digital anonymity and the law – Tensions and dimensions*, T.M.C. Asser, The Hague, 2003, 221.

<sup>38</sup> Identify theft is defined as the case in which personal details have been stolen and are used illegally. In most cases identify theft happens through the method of *phishing* (criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication) or *pharming* (a hacker's attack aiming to redirect a website's traffic to another, bogus website).

<sup>39</sup> Other possible threats are glorifying activities such as drug taking or excessive drinking; encouragement of violent behaviour such as ‘Happy Slapping’; physical harm to young people in making video content, such as enacting and imitating stunts and risk taking activities such as playing ‘Chicken’ on railways; leaving and running away from home as a result of contacts made online.

<sup>40</sup> See for the *Joint Statement on Key Principles of Social Networking Safety*, declared by U.S. Attorneys General and MySpace on 14<sup>th</sup> January 2008, where the website agreed to implement such ‘age locking’ tools for new profiles so as minors will be locked into

tool that can bypass some of the aforementioned limitations of age verification *per se*, as it will only define as threshold the over/under eighteen years old.<sup>41</sup> This solution can be useful also to hinder grooming as children personal data (and also photographs, address, etc.) cannot be seen by over eighteen,<sup>42</sup> but it could not limit cyber-bullying, if the bully is in the same age group.<sup>43</sup> In the latter case, the provision of a ‘report an abuse’ button could be added in the site design, so as to give users the possibility to report any uneasy situation including cyber-bullying, pornography or unauthorised use. This could help in drafting a rating system based on the experience of users, (though the use of children as guinea pig would not be borne as acceptable).

However, the previous solutions are mainly on voluntary basis, as they are default settings coded in the software written for the social networking site (or they are included in clauses of the codes of conduct). In other words, these rules are applied by social networking site as long as they have incentives to do it. On the one hand, the accountability and the sensibility to acceptable children security level can enhance the usage of the website, as for instance parents will not impede to their children to access and participate to such websites. On the other hand, it must be underlined that social networking sites earn revenues through their activity, though services provided to users are (generally) free. As a matter of fact, revenues come primarily via third party advertising served to users.

For instance, a privacy policy can state that: “*We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you.*”;<sup>44</sup> however, this leaves open the question of when exactly

---

the age they provide at sign-up while 18 years old and older members will be able to make changes to their age as long as they remain above the 18 years old threshold.

<sup>41</sup> It must be said that any user can create a fake online profile, so as to get into the adult or children limited space, however, in such networks the evidence given by photographs and alike could clearly give information about real age or at least instil some doubts.

<sup>42</sup> This is also more efficiently achieved through other technical solutions, i.e. restricting ‘friend requests’ to only those who know email address or last name of the children, imposing ‘friends only’ group invite as mandatory (or as default) preference in profiles, etc.

<sup>43</sup> This is usually the case, as bullying starts in school, mostly among classmates.

<sup>44</sup> This example is taken by Facebook privacy policy, available at <http://www.new.facebook.com/policy.php?ref=pf>.

the site “believes” that you wish to share your information.<sup>45</sup> In practice, the website would allow third party advertisers access to its site and users, permitting them to profile users and send targeted advertising.<sup>46</sup>

On a completely different perspective, we should also take into account children perception of such interventions. As a matter of fact children and young people would interpret those devices as restrictions to their social networking activities. This would be self-defeating if children reaction will be to leave security-sensitive website and participate in other sites where more lax operating restrictions are available. The issue, still without easy solutions, is how to create sensible online policies without encouraging kids to operate completely surreptitiously in a “digital underground”.

## VI. CONCLUSIONS

A conclusion that can be drawn from the preceding case study is that any policy aimed at protecting children, either from illegal and harmful content or from other possible online risk, due to the nature of the subject-matter, should be of a multi-faceted nature.

On the one hand, in order to achieve an adequate level of effectiveness, several measures and actions should be combined in a complementary way, such as creating reporting facilities, empowerment of children as users of these technologies, self-regulatory elements and structures for cooperation between different stakeholders.

On the other hand, we should not overestimate the aforementioned solutions. For instance, technical devices will always suffer from inherent limitations and can be circumvented. A different factor that, instead, can last for a lifetime and can build a better online environment is children education.

---

<sup>45</sup> See for a deeper analysis of privacy issues concerning social networking sites, L. EDWARDS and I. BROWN, “Data control and social networking: irreconcilable ideas?”, cit., 14.

See that in the case of anonymised data this could be possible, as for instance Facebook privacy policy clearly admits: “Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as aggregating how many people in a network like a band or movie and personalizing advertisements and promotions so that we can provide you Facebook. We believe this benefits you. You can know more about the world around you and, where there are advertisements, they're more likely to be interesting to you. For example, if you put a favourite movie in your profile, we might serve you an advertisement highlighting a screening of a similar one in your town. But we don't tell the movie company who you are.”

<sup>46</sup> See F. CASAROSA, “Privacy in search engines: Negotiating Control”, on file by the Author.

An important and ever-increasing role should be given to teaching children how to be good cyber-citizens and how to identify and report online threats (predators, bullies, scam artists, etc.). Moreover, as children are now more savvy and sensible about online threats, it is even more important – for institutions, parents and carers – to keep being vigilant about online safety education and etiquette, providing always better and more accountable ways to give children lessons about sensible online behaviour and relations.

# **THE CONCEPT OF NETWORK NEUTRALITY IN THE EU DIMENSION: SHOULD EUROPE TRUST IN ANTITRUST?**

Oles Andriychuk

## **I. NETWORK NEUTRALITY IN THE EUROPEAN CONTEXT**

### *I. Introduction*

Ontologically, 'network neutrality' is a political and not a legal term. It has been introduced in the legal literature by US antitrust scholars and is by now well established and consensually used. It constitutes the premise of original destiny of the telecommunications infrastructure as a conduit of all relevant data with (virtually) no interference of incumbent into this process. Because of its political roots, it does not convey the literal meaning of neutrality. Most actors on both sides of the debate agree that not every data has to be transmitted without any prioritisation. For instance, the succession of e-mail, banking and security services is always prioritised over other internet applications.

After two decades of the Community liberalisation policy in the telecommunications area, the domestic European markets have become relatively integrated and disclosed. This gives the chance for the world wide leaders of the electronic communications industry to enter into the regulatory homogenous and rapidly growing European telecommunications environment without needing to comply with the twenty-seven different administrative regimes of the EU member states. The opening of the European telecommunications industry is a long-term process, which has to be seen along its three dimensions; that is, incumbents *versus* new entrants, domestic telcos *versus* their European *vis-à-vis*, and European telcos *versus* foreign competitors. The history of the interactions between these three groups of telecommunications actors shows many examples of their fierce contest in. and mostly for, the markets. Every telco strives to promote its own commercial interests, often simultaneously supporting different, even controversial, theoretical approaches in the different markets: from preserving strong regulation to complete de-regulation; from maintaining a monopoly position to fostering competition; from hard protectionism to libertarian market disclosure. The position of the companies depends on their status in each relevant market: as incumbents or as new entrants; domestic or European; European or foreign. However, there is an area in which they reach practically unconditional consent: they are unanimous in relation to network neutrality. Among the companies which represent the opposite side of this theoretical debate, the situation

is similar as well.

Until the moment of rapid growth of internet technologies, which provides high speed traffic over the new FTTx networks -and, consequently, the transmission of large-sized files and applications-, the discussion on network neutrality had only a theoretical dimension. With the fast development of Voice over Internet Protocol (VoIP) technologies, Internet Protocol Television (IPTV), video-on-demand and movie-downloading services (otherwise large-sized files and applications), the amount of traffic over the network has been growing exponentially. Concurrent to this process, there has been a substantial development of the infrastructure, which can now be managed gradually by Internet Service Providers (ISP). In practice, this means that ISPs, who are often at the same time the owners and administrators of the networks, can 'range' the traffic speed of different internet applications.

Because of digital convergence and systematic elimination of the frontiers between infrastructure, platform and content of the internet, many ISP are beginning to consider launching for their users the provision of different kinds of content services under different traffic speed (two-tier Internet). Concurrently, some big internet companies are launching their own wired and wireless networks, like Google in San Francisco.

As soon as ISP acquired the technical abilities to 'range' the traffic of different applications and, most importantly, of different content providers, they started to consider the possibility of providing high-speed premium services for content operators interested in instantaneous delivery of their services. This option is particularly important for such time-sensitive applications as broadcasting of live sports events, video conferences and some other communication services. Under such conditions, internet speed became a *killer application* for attracting new clients and gaining substantially higher revenues. There are two hypothetical models of applying this premium speed services: on one hand, assigning such extra-speed capacity to other content-providers for additional fee and, on the other hand, vertical integration of ISP with certain content-provider and offering content services on its own.

The merely technical capability of ISP to charge their clients -to be understood as charging on both sides of traffic, that is download or consumers and upload or content providers- brought on commercially justifiable apprehensions in the content-providing internet industries. Services which content providers have traditionally received by simply paying for upload speed and data capacity at the upstream level may now only be obtained by these companies for additional payments at the

download level, depending on the real amount of users. This scenario appears to be only hypothetical, since nobody is allowed to *degrade* the speed of some particular content or application. Besides, it would never be possible from the political or *freedom of speech* and commercial or *cannibalisation* of existing business model points of view. However, the growing popularity of premium speed services would indirectly leave in the cold those content-providing companies who will continue to rely upon merely average 'non-discriminatory' speed of data transmission.

So, does prioritisation actually mean discrimination? The answer to this rather philosophical question definitely depends on the initial position of the inquirer. As it always happens with debates in the area of competition law and regulatory policy, each party tries to obtain the *cheval de bataille* of its rectitude; namely, benefits for consumers and improvement of the general economic welfare.

This situation impelled content providers to launch a wide-ranging political campaign on network neutrality, with the intent to preserve the existing *status quo*, by means of introducing broad public discussions and implementing the relevant legislative framework. The epicenter of these debates was initially situated in the United States, where this topic received tremendous public coverage and scientific conceptualisation. However, nowadays, the network neutrality concept is becoming increasingly more popular in other jurisdictions, particularly in the European Union and Japan, where these debates are still in their infancy.

Leaving aside such controversial issues as the level of censorship, privacy, and copyrights protection of the transmitted content, local internet service providers are apparently aware of their customers needs, at least as much as world-wide content providers are. Therefore, they will never jeopardise the services of high-speed data delivery by blocking or slowing down certain applications. However, one must recognise that, with some minor exceptions, providers of broadband internet services are usually monopolists in the local markets and their dependence upon content-creating companies is significantly less than *vice versa*. Does this mean that their business practices need to be regulated by sector specific instruments, such as compulsory access or neutral traffic requirement, or are the traditional mechanisms of *ex post* competition law reasonable and sufficient in the present context? What is the legal difference between the American and European approaches to network neutrality and where exactly is it situated? These are two central questions that this paper will attempt to tackle.

## 2. *Jurisdictional concerns, quo warranto*

Telecommunications law was not originally supposed to have a European Community dimension. The founding fathers of European integration laid down *prima facie* explicit clauses in the legal foundation of the European Community, reserving telecommunications to the national regulatory regimes. Indeed, at the time, the social and political status of telecommunications was considered as one of the strategic domains of internal affairs.

Thus, Article 86 of the Treaty Establishing the European Community stipulates:

In the case of public undertakings and undertakings to which member states grant special or exclusive rights, member states shall neither enact nor maintain in force any measure contrary to the rules contained in this treaty, in particular to those rules provided for in Article 12 and Articles 81 to 89.

Undertakings entrusted with the operation of services of general economic interest or having the character of a revenue-producing monopoly shall be subject to the rules contained in this treaty, in particular to the rules on competition, in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them. The development of trade must not be affected to such an extent as would be contrary to the interests of the Community.

The Commission shall ensure the application of the provisions of this article and shall, where necessary, address appropriate directives or decisions to member states.

Neither literal nor historical interpretation of these provisions gives us a ground for questioning the original intentions of the member states. The initial political will consisted in reserving the telecommunications policy for domestic regulation.

Nevertheless, in the course of time, the interpretation of Article 86 has been hermeneutically moved towards substantial an expansion of the Community's competences in the present domain. Accordingly, teleological and systemic modes of interpretation provide a clear picture of the 'genuine mission' of the treaty and classify telecommunications as one of the most important *European* policy. The European Commission has been one of the most active proponents of such a shift of paradigm in the evaluation of the status of telecommunications policy in the economic

constellation of the EC. This pro-European approach was ultimately legitimised by the judicial opinions of the Community's courts, *videlicet* in the relevant case law.

Technically, the self-contradictory provisions of Article 86 might be interpreted in different ways, both in favour and against of the parties to the present dispute. Under these circumstances, the decisive factor is to be found in the general purpose of European integration, which is based on striving to complete the single internal market; that is, on Articles 15, 26, 47 § 2, 49, 80, 93 and 95. This aim serves as a common denominator for the arguments of both parties. Not surprisingly, the reference to the overall value of market integration sorted all things out and ended up presenting the telecommunications policy as genuinely European.

### 3. *Libéralisation! Harmonisation! Concurrence!*

The European telecommunications policy was supposed to be governed by three major principles: *liberalisation*, *harmonisation* and *competition*. These three maxims directly correspond to the three core European meta-tasks; namely, completing the internal market, setting out Community-wide uniform social and economic regulatory system, and fine-tuning the optimal competitive institutional environment.

It is noteworthy that, although these three objectives all constitute important elements of European economic welfare, they also quite often contradict themselves. The main problem lies in their ontology and methodology. Traditional *ex post* competition rules and antitrust law are graduate and predictable. They provide for incumbents substantial amount of legal certainty. In contrast, the *ad hoc* nature of regulations, which constitute the main instruments of liberalisation and harmonisation, are rather based upon the rationale *exitus acta probat*.

There are philosophical doubts as well about the correctness of the term *liberalisation*, which in this particular context would actually mean "*liberalisation through regulation*" and not "*liberalisation from regulation*". From the perspective of negative freedom, such a formula constitutes a *contradictio in terminis*. This being said, proponents of a positive conception of freedom consider volitional interference and *creativity* as an indispensable component of any genuine form of freedom. In the context of the European telecommunications regulatory regime, *liberalisation* consequently means an aim, whereas the methods of reaching this aim are far from liberal and include, for instance, limitation of profitability, common carriage obligations or compulsory access.

The ontological legacy of European telecommunications based upon original state ownership provides an additional, although rather rhetorical, argument for regulatory interference by the Commission. In the course of the privatisation of most European telecommunications giants, the permanent implicit emphasis has been put on the fact that the entire network infrastructure has been built by the sweat of nation's brow; a consideration, which can be euphemistically interpreted along the lines that the industry will continue to be regulated at least for a while.

This is particularly important since, under the current European regulatory regime, even telecommunications companies without significant market power -as opposed to the rules defining the dominant position in *ex post* competition legislation- may be obliged to provide in certain cases for their competitors adequate access to infrastructure and services. The Commission recognises the exceptional character of such compulsory remedies, but proposes to preserve this practice in the new regulatory framework for telecommunications. Furthermore, in order to ensure the consistent application of this condition and to avoid the imposition of inconsistent obligations without a market analysis, it is proposed to harmonise this procedure on the Community level. Supposedly, this would prevent the risk of over-regulation and a fragmentation of the internal market through the imposition of inconsistent obligations. The procedure of cooperation between Commission and NRA is provided by Article 7 of the Directive on a common regulatory framework (2002/21/EC). It requires NRA to conduct a national and Community consultation on the relevant regulatory measures they intend to take. The Commission may issue comments and, under certain circumstances, block the proposed regulations.

#### 4. *European policy of limited profitability*

On the road to privatisation of previously state-owned telecommunication companies in Europe, the most popular form of regulation was the limitation of the investment rate. This basically implied post-selling state's control over incumbent's tariff policy by means of requirements to restrict the scope of its returns and aggregate profitability. According to these conditions, commercial incentives for telecommunication companies and their subsidiaries should be limited by general revenue caps. This presupposes the possibility to gain solely a 'proportional' margin of profits, which should take into account the interests of direct, potential and (maybe) even hypothetical competitors.

Limitation of profitability ratios is a rather objectionable and controversial instrument of telecommunications policy. From a theoretical perspective,

it raises substantial doubts about the appropriate functioning of the free market, by not only restricting the genuine intention of service providers to render access to facility at the highest possible price but also confining the inherent business intentions of the incumbents to innovate and improve the quality of the telecommunications services.

Since the policy of limited profitability applies for the most part uniformly to the whole industry, often without appropriate differentiations between the various segments of telecommunications businesses, the sporadic benefits of such regulatory interventions are considerably degraded by economic damages, which are raised from unnecessary market limitations in other allied areas of the industry. Furthermore, these restrictions are quite often applied to markets where the incumbent neither abuses nor even holds the dominant position or where the competition functions well and there is no rational necessity whatsoever for regulatory intervention by public authorities.

Because of the complexity and the rapid changes that occur when offering different services inside the telecommunications industry, it would be unrealistic to predict the existence of a well-differentiated ranging system of regulation, which fully takes into account the specificity of the various markets and submarkets; thereby, providing mobile and efficient operational regime.

In addition, the limited profitability policy of telecommunication companies does not bring any substantial benefit to the consumers. These interventionist regulatory mechanisms may serve only for reaching short-term and fairly marginal advantages, because in the long and middle-term perspective the lack of incumbent incentives to innovate together with their intentions to structurally optimise existing formats of business in order to adjust to regulatory pressure cannot lead either to establishing of workable competition model within internal market or to improving services. Under the present system, a large amount of incumbent efforts are re-directed to a sophisticated parcelling into different entities or affiliated enterprises in order to comply with legal requirements,<sup>1</sup> virtually sharing gained profits between different pockets of the same jacket.

Another important disadvantage of limited profitability rules in the

---

<sup>1</sup> This remark does not intend to contest or otherwise cast doubts on the probable existence of some genuine competition between companies owned by the same person (*e.g.*, by accounting separation). On the contrary, there are sufficient evidences to believe that, in some industries, ownership does not play decisive role with regard to competition (*e.g.*, rivalry for audience among TV-channels, which legally belong to one media holding).

telecommunications sector is that they deform the fundamental notion of regulatory policy, impelling beliefs upon dependent companies about the constant character of such well-disposed regulatory climate on the relevant market. The legacy of regulatory over-protection decreases abilities of dependent companies to compete under the conditions of workable competition. In return, it incites them to lobby the legislation and support the general political atmosphere in favour of the conservation of the current state of affair in the industry. One can easily find persuasive arguments for regulatory protection, especially if the success or even mere existence of the dependent companies is at stake. In this situation, there is direct evidence that, by definition, the provisional character of each *ex ante* regulatory interference slowly but surely transforms into a permanent state of play for the whole telecommunications industry.

For all intents and purposes, regulation plays the part of first violin in many domains of public community affairs, including those related to the economy. It is indispensable *inter alia* in the relations of establishment and registration, fiscal and financial control, as well as in a range of other inspecting and administrative matters. Furthermore, it is inevitable in securing performance of common carriage through the provision of universal services. However, the primary task of regulatory policy in the area of market fine-tuning is to establish, improve or modify competition in the relevant market(s) and, in no circumstances, to substitute it by nearly command-and-control practices, such as the policy of limited profitability.

The references of the proponents of the limited profitability policy are based to a large extent on the fact that newly established competitive markets of telecommunication services are dependant upon regulatory interference, as they would otherwise be unbearably pressured by the incumbents and forced to abandon the market. This presumption is increasingly gaining the status of an axiom in the industry. Another reasonable argument is based upon the widespread -although rather deductive- experience of abusive monopolistic behaviour of the incumbent in the presumably unregulated environment. In an ideally modulated world, competition in the network industries is a rather temporal issue, considering that monopolisation of the market is almost indispensable in the end. As the common adage goes, the winner gets all. Under these circumstances, the successful incumbent would be motivated to operate according to the paradigmatic winner-gets-all formula. This is precisely the reason why both *ex post* (competition laws) and *ex ante* (sector specific regulations) regulatory policies are called upon.

As a general rule, the most important instrument for public regulation of

the market economy appears to be competition law. Because of its existential universality and legal conformity, this tool is precisely considered as a commonly acceptable *raison d'être* of moderate and predictable market regulation. Competition law has its well-elaborated jurisprudence; it is based upon judicial principles and case-law. In legal reasoning, there is much more about law here, then about competition. Hence, competition law is an instrument, which provides a substantial amount of legal certainty and refers to principles of law or at least does accept them as a value.

The *ex ante* regulatory instruments of market regulation are not characterised by predictability and legal continuity. They are fully tied to the political context and they are adopted by executive authorities as rules rather than as principles. *Ex ante* instruments are much more flexible and easy to change. Their mission as regulators of competition lies in establishing short-term contextual tasks in accordance with everyday political necessity. The legal nature of *ex ante* regulation is *consequentialist* concerning the results achieved in the market. Its algorithm consists in the claim that sector specific regulations are temporal tools for matching market failures, which cannot be fixed by *ex post* regulation. In course of time of their legal validity, they may directly contradict competition law as *ex post* regulation. Yet, they would still apply in spite of this formal discrepancy with competition law and even the plausible higher place occupied by the latter in the formal legal hierarchy.

##### 5. *Local loop unbundling*

The European policy in the area of network neutrality has to be seen in close connection to the approach of the Commission towards the issue of local loop unbundling. The regulatory regime of the latter may be transposed in the future to the former, since both are directly related to the regulation of the appropriate managing of networks and both eventually provide very high obligations for the incumbents.

Local loops constitute physical wired intermediary between telephone exchange central offices and end-users telecommunications lines. The essence of local loop unbundling policy is based on granting to incumbent competitors the fair and non-discriminatory use of the facility of monopolist. The technical characteristics of local loops do not permit their duplication under economically reasonable terms. Naturally, the opinions of the main industry players are divided, depending on the factual power in the markets of networks interconnections. As a result, companies that possess local loops -virtually, always monopolistically- are insisting upon their genuine property rights to operate their own facilities, whereas

new entrants and companies who do not have well-developed network infrastructure refer to their right to compete and ask for the permission to use local loops under the same conditions as incumbent affiliated companies do.

Another more radical variant of local loop unbundling consists in *bit stream access*, which essentially is an entrance to the market of electronic communications made by a company which possesses no infrastructure equipment at all. Neither the current nor the reformed European telecommunications regulatory framework does explicitly maintain compulsory provision of bit stream access. However, according to the Directive on access and interconnection (2002/19/EC), incumbents are obliged to provide different forms of access under transparent and non-discriminatory terms and conditions. Hence, a proactive interpretation of this provision may lead to compulsory access to the network by competitors, if such access has been made for at least one of them. According to Article 1 § 3 of Regulation (EC) No 2887/2000 on unbundled access to the local loop, “this regulation shall apply without prejudice to the obligations for notified operators<sup>2</sup> to comply with the principle of non-discrimination, when using the fixed public telephone network in order to provide high speed access and transmission services to third parties in the same manner as they provide for their own services or to their associated companies, in accordance with Community provisions”.

The practice of the Commission demonstrates its willingness to foster innovations in the bit stream markets, in particular outside of densely populated metropolitan areas. National regulatory authorities are required to notify their market analysis with regard to several pre-defined markets to the Commission and one of these markets is the market of bit stream access.<sup>3</sup>

One of the most appropriate solutions for this dilemma may be provided by the market itself; in particular, rapidly growing wireless technologies. In the predictable future, wireless connection may become an appropriate platform for high-speed transmission of data. This is already the case in the most technologically developed local communities around the globe. The economic potential of wireless communications is enormous. According to the Commission, the total value of services that depend already today on use of the radio spectrum in the EU exceeds €200 billion.

---

<sup>2</sup> Notified operators are those operators that hold significant market power.

<sup>3</sup> In 2006, the Commission approved the decision of the German regulator *Bundesnetzagentur* to open up broadband markets, including very high-speed internet access (VDSL) with regards to Deutsche Telekom.

Wireless has been a strong driver of economic growth of Europe.<sup>4</sup>

Wireless technologies constitute an effective substitute to more traditional electronic communications. Their intensive usage would help solving existing bottleneck problems in the area of local loop interoperability. There are reasonable market premises to believe that, instead of strict compulsion to open the access for the local loops, the regulator could re-direct its efforts to promoting wireless technologies, fostering new entrants to adopt new business strategies, which would not only establish competition in the markets, but also promote innovations for the benefits of consumers. This approach would be particularly appropriate in the light of the Commission efforts to liberalise the spectrum policy and to bring its regulation at the Community level.

Since the Commission proposal for review of the European electronic communications framework is focused on empowering market players and giving them the necessary legal certainty to exercise their role of innovators, it would be both effective and consistent to provide them with the regulatory prerequisites for such incentives; namely, to restrict the commonly used practice of local loop unbundling and impel new entrants to look for their way to success *via* new wireless technologies rather than by free riding on existing facilities.

## II. EUROPEAN LAW OF ELECTRONIC COMMUNICATIONS

### I. *Present-day regulatory regime*

The legislative failure to include network neutrality provisions into the Communications Opportunity, Promotion and Enhancement Act of 2006 gives a glimpse of the preliminary state of affairs in the United States. This is not the case for Europe. Indeed, the network neutrality issue is neither settled nor properly articulated in the European context. The debates over telecommunications in the EU take place under another methodological apparatus, with different priorities and somewhat shifted accents. Then again, it resembles the US situation in the clear-cut definition of the European opponents and adherents to network neutrality. The former contains most of ISPs, regardless of their legal property relation to the networks. The latter are united around the most powerful and ambitious content suppliers.

---

<sup>4</sup> See: V. REDING, *The Review 2006 of EU Telecom Rules: Strengthening Competition and Completing the Internal Market*, Annual Meeting of BITKOM, Brussels, Bibliothèque Solvay, 27 June 2006; which expresses the views of a member of the European Commission responsible for the information society and the media.

Despite the strong commitment of the main European regulatory player - that is, the Commission- to proactive telecommunications policy, the opponents of network neutrality are in a more advantageous position, since they have to merely need to advocate preserving the *status quo*; namely, the application to presumably discriminatory conduct of ISPs of *ex post* antitrust rules. Conversely, the proponents of network neutrality are called upon to persuade the European legislator of the necessity to adopt explicit *ex ante* regulatory measures. However, taking into consideration the power of public opinion upon the European decision-making process, the perspectives of network neutrality legislation appear to be quite likely. Under these circumstances, consumer welfare constitutes an *ultima ratio* for future network neutrality debates in Europe.

Innovations and investments have another 'golden share' in this discussion. One of the best ways to attract new investors into the telecommunications market is to demonstrate its profitability, regulatory benevolence and potential for future evolvment. Over the last years in the case of the EU, and decades in the case of the US, the reference to efficiency often became the decisive factor during administrative scrutiny and judicial hearing. The post-Chicago approach to the analysis of monopolist economic behaviour and its consequences for the market is currently applied upon an almost consensual agreement of all stakeholders. Which regulatory model -liberal or proactive- will create favourable preconditions for long term investments into the new technologies? The convincing answer to this question predetermines the attitude of regulatory authorities to network neutrality.

Antitrust law is the most appropriate *ex post* regulatory watchdog for European telecommunications -particularly in the area of content / application gradation- because competition in the markets of internet services provisions is already secured and created by other EU regulatory tools; namely, the European regulatory framework for electronic communications and European audiovisual policy. These instruments provide a sufficient basis for opening markets and the additional network neutrality clauses will bring *de facto* regulatory duplication. If the aim of *ex ante* regulations is to establish a competitive environment in the markets and not to protect competitors, the network neutrality rule is unnecessary. Indeed, it does not guarantee horizontal competition between the ISPs, but only impose on them non-discrimination duties in relation to their vertical relations with content providers. The only *ex ante* regulatory tool which is really essential for establishing some competition between ISPs is the current European policy of local loop unbundling and bit stream access. However, these measures significantly infringe upon essential property rights of the network incumbents. Then again, since they are

already established, one might as well take into account their positive aspects for the European economy. The legal and economic evaluation of these premises constitutes an important aspect of the present contribution.

At the present stage of evolution of the telecommunications market, the networks represent the biggest 'bottleneck' for content distribution. Therefore, the attraction of investments into their deployment has to be seen as a major regulatory priority. Following the liberal postulate according to which softer regulation is a stronger regulation, the possibility to gain vast revenues from a 'gatekeeper' position is a substantial stimulus for new investors. The widespread argument of inefficiency of the networks duplication still plays an important, but no longer decisive, role in the modern telecommunications economy, especially taking into account the vigorous potential of the next generation wireless networks. This contribution demonstrates how exactly market failures can be effectively solved by antitrust procedures in the relevant areas.

As a result of fast technological evolution and a growing juxtaposition in a number of communication areas, a draft of the new telecommunications framework has been launched at the beginning of 2000. Because of a rapid convergence among the three previously almost not at all interconnected sectors that are telecommunications, information technology and the media, the decision has been made to cover all of them through a single regulatory regime. This new framework included the regulation of both telecommunications and broadcasting aspects of communications, which previously had been regulated separately. However, the new regulatory regime of communications did not include either content services providing editorial control or information society services, which do not mainly consist in the transmission of signals on electronic communications networks. Apart from the explicit exclusion of audiovisual services, the new electronic communications proposal provided no coverage for the regulation of telecommunications equipment.

The new regulatory framework came into force on 25 July 2003. Initially, this new package consisted of five directives: the Directive on a common regulatory framework (2002/21/EC), which lays out the main aims and procedures for an EU regulatory policy in the area of the provision of telecommunications services and networks; the Directive on access and interconnection (2002/19/EC), which regulates the access to and interconnection of networks on operators with significant market power; the Directive on the authorisation of Electronic Communications Networks and Services (2002/20/EC), a mechanism to establish a new system of general authorisation, under the provisions of which directive

national regulatory authorities can no longer issue licenses but only establish a general authorisation for all telecommunications services; the Directive on universal service and user rights related to electronic communications networks and services (2002/22/EC), which provides a minimum level of telecommunications services to European consumers; and, finally, the Directive on privacy and electronic communications (2002/58/EC), stipulating the rules for protection of personal data and privacy.

One of the main reasons to propose the framework was to harmonise the communications legislation. In addition to this packages, the Directive on competition in the markets for electronic communications services (2002/77/EC), the Decision on a regulatory framework for radio spectrum policy (678/2002/EC), the Decision on the minimum set of leased lines with harmonised characteristics and associated standards (2004/641/EC), the Decision establishing the European Regulators Group for Electronic Communications Networks and Services (2002/627/EC) and the Recommendation on relevant markets (C (2003) 497) have added latter on. This paper does not review all the provisions of the relevant Regulatory Framework directives; instead, it focuses on specific aspects of the directives, which are related to network neutrality.

At the current stage of the EC telecommunications development, one needs to acknowledge the general political will to move towards greater application of antitrust *ex post* European principles. This gesture is still far from the consensual recognition of the competition law rationale's dominant position in the area of telecommunications. On the other hand, it might be interpreted as a manifestation of the completion of the first proactive regulatory stage in the infrastructural liberalisation.

## 2. *Compulsory infrastructure access*

In accordance with the current European regulatory model, compulsory access to the network infrastructure can be justified as a means to increase competition. The Directive on access and interconnection (2002/19/EC) obliges network operators with significant market power to meet reasonable requests for access to and use of networks elements and associated facilities, stipulating that such requests should only be refused on the basis of objective criteria such as technical feasibility or the need to maintain network integrity. In cases where access is refused, the aggrieved party may submit the case to the dispute resolutions procedure referred to in Articles 20 and 21 of the Framework Directive (2002/21/EC). However, national regulatory authorities are required to find a proper balance between the short-term interests of the new entrants and their incentives

to invest in alternative facilities that will secure more competition in the long-term.

Price control constitutes one of the most important regulatory instruments of compulsory access. In the markets where the competition is not well-developed, the incumbents are prohibited from imposing excessive prices and using price squeeze tools for eliminating competition. The Directive on access and interconnection gives to the national regulatory authorities the necessary rights for appropriate price control, such as cost accounting systems and undertaking an annual audit to ensure compliance with that procedure.

It is noteworthy that the national regulatory authorities are not limited in their imposition of compulsory access provisions (exclusively) to situations where a company dominates the market.<sup>5</sup> Such obligations go far beyond the *ex post* competition principles and along with liberalisation bring disincentives for incumbents to innovate and expand their networks.

The new phase of telecommunications policy illustrates the Commission's willingness to reassess the existing electronic communications regulatory framework. The main impetus for a reform came from the fast-changing nature of the telecommunications structure, from the deep convergence of various interrelated services -namely, the operation and deployment of the network infrastructure, access services, entertainment and content provision- and from the multilevel interdependence between them.

During public consultations, many incumbent operators and some national authorities considered that the regulatory framework should foster more investment and they called for a major reform. Nevertheless, some have pleaded for either withdrawal of sector-specific regulation or regulatory holidays for major investments that made significant financial injections into structural renovation of their networks.

The Proposal covers the area of common carriage services provision. In the Commission's opinion, because of the fact that the fast technological progress significantly changed the conditions under which common carriage service rules operate, and keeping in mind a deep infrastructure deployment and establishment of alternative networks, these services need

---

<sup>5</sup> Article 3 § 2 of the Directive on access and interconnection stipulates that "where, as a result of [...] market analysis, a national regulatory authority finds that one or more operators do not have significant market power on the relevant market, it may amend or withdraw the conditions with respect to those operators, in accordance with the procedures referred to in Articles 6 and 7 of Directive 2002/21/EC (Framework Directive)".

substantially less regulation from the member states. Conversely, in order to apply common European standards to such services, it is proposed that the common carriage services obligations of the incumbents must be as proportionate and transparent as possible. The document proposes to introduce a deadline for reviewing national common carriage rules and give a spur to liberalise the national markets and introduce competition within newly opened segments of the telecommunications market.

One of the most important and controversial proposals of the Commission is related to the provision of a universal service. The current EC regulations on universal services are based on the 'classic' model under which telecommunications companies may often provide both access to the network and voice communication services. In the Commission's opinion, such a vertical integration model where the incumbent provides services of access to network and voice communications may harm -or, to put it in more appropriate terms, "not foster"- the competition within the internal market. As a result, it offers to introduce separate obligations on providers of access infrastructure and on providers of services. One of the main reasons for this legal transformation lies in the fact that the Commission foresees a rapidly growing interconnection of the different services and, consequently, some potential harm for the internal market as competition *for the market* would prevail over competition *in the market*.

According to Article 3 of the Directive on competition in the markets for electronic communications services (2002/77/EC), "member states shall ensure that vertically integrated public undertakings which provide electronic communications networks and which are in a dominant position do not discriminate in favour of their own activities". The Directive on access and interconnection (2002/19/EC) stipulates that telecommunications companies with significant market power are obliged to operate in accordance with the principle of non-discrimination and ensure that undertakings with market power do not distort competition, especially where there are vertically integrated undertakings that supply services to undertakings with whom they compete on downstream markets.

Hypothetically, the attempt of the Commission to regulate the telecommunications industry in such interventionist fashion might be justified by the goal to reach some efficiency gains for the European market. However, this policy may also lead to a decrement of the general level of legal certainty in the business environment and negatively reflect upon the intentions to invest into the future development of the infrastructure. As of today, it is still hard to predict the kind and methods of regulatory measures, which may be applied in order to impel the

incumbents to give up certain part of their business. This appears even less likely if one keeps in mind that the control over the network allows them to carry on a wide range of legitimate economic leverages.

The spirit of this proposal is not consistent with the broad economic studies in the area of *ex post* competition law, because the political, industrial and academic discourses in the antitrust domain reached almost unanimous consent upon economic efficiency of the vertically integrated business. The possible remedy for vertically integrated companies in competition law may be applied solely in the course of a merger's approval. Vertically integrated companies may undergo an additional responsibility for abuse of their dominant position, but such a responsibility may not concern compulsory separation of the incumbent, since it is the consequence of *behaviour* but not the mere *status* of the company *per se*.

### 3. *Network neutrality in the new regulatory framework*

Another domain which the reformed regulatory framework proposes to cover is that of network neutrality. The term has been created in the US public debates by proponents of the current model of relations between telecommunications companies and providers of internet content. The rationale behind network neutrality is based upon a prohibition of 'double charge' for providing internet content to the end-users. The idea of launching the network neutrality movement is based upon the eventual threat for internet companies that aroused from the intentions of internet providers to establish prioritised services for users or companies who are willing to pay more for a substantial speed increment of data transmission.

The Commission's regulatory proposal maintains a quite ambivalent position in this regard and states that, "in Europe, the regulatory framework allows operators to offer different services to different customer groups, but does not allow those who are in a dominant position to *discriminate* between customers in similar circumstances". The effective consequences of the distinction enshrined in this formula will, in all likelihood, be established exclusively on a case-by-case basis. The Proposal contains an important clause which empowers NRA to establish minimum quality levels for transmission of data *via* networks, particularly to avoid a situation of degradation of the quality of the service to an unacceptably low level. The Commission considers that any dispute raised among parties concerning the different interpretation of network neutrality principles should be resolved in accordance with the rules of *good faith* and refers to Article 5 § 1 of the Access Directive; according to which, "in an open and competitive market, there should be no restrictions that prevent undertakings from negotiating access and interconnection arrangements

between themselves, in particular on cross-border agreements subject to the competition rules of the treaty”.

The possibility of application of the provisions of non-discrimination in the context of network neutrality will depend on an infinitude of eventual interpretations of Article 10 § 2 of the Directive on access and interconnection (2002/19/EC); which stipulates that “obligations of non-discrimination shall ensure, in particular, that the operator applies equivalent conditions in equivalent circumstances to other undertakings providing equivalent services, and provides services and information to others under the same conditions and of the same quality as it provides for its own services, or those of its subsidiaries or partners”.

The proponents of network neutrality interpret these provisions as a prohibition to prioritise the transmission of different services and applications, emphasising that in case of vertical integration of the infrastructure and content providers the conditions for premium traffic speed should be automatically transferred to other content providers. However, the incumbents would reasonably refer to the non-discriminatory character of premium speed services, since each company can receive access to such facilities under equivalent conditions. Hence, the abovementioned provisions of the Directive on access and interconnection regulate the relationship of network operators and the new entrants, electronic communications companies, who strive to operate within the same infrastructure.

Even taking into account the highly growing convergence of technologies and applications, these conditions can apparently not be directly applied to the relations of network operators with content providers. The evolution and development of the concept of network neutrality, its ontological essence and legislative regulation, both in the US and EU, will be scrutinised below.

The Commission analyses three potential scenarios for the development of the telecommunications regulatory framework: the removal or restriction of sector-specific regulation; the adoption of an ‘open access’ model for new network structure; and, lastly, no change to the regulatory framework.

The first or ‘free market’ model is characterised by its eventual advantages for the current incumbents and a substantial increase in the level of economic predictability and legal certainty. Besides, the removal or restricted application of *ex ante* regulation may provide an incentive for long-term investment and make European markets more attractive to trans-national capital. This option envisages the application in the

telecommunications area of *ex post* competition policy rules without considerable sector specific measures.

The biggest disadvantage of this regulatory approach lies in its disintegrative character. The removal of the uniform European regulation would authorise *status quo* in the European telecommunications, currently characterised not only by different levels of technical and structural development but also by diverse approaches with respect to liberalisation, often benefiting from a privileged (quasi-)national legal status granted by member states.

In addition, the removal of *ex ante* regulation in a market where the incumbent operator benefits from a dominant position is likely to slow down the level of effective competition and to disadvantage consumers. The rapid growing importance of the communications area in digitally-oriented economies demonstrates that predictable long-term dominance does not constitute the exclusive condition for extensive investments in the new generation networks.

The second option is diametrically opposed to the removal or restriction of sector-specific regulations. It consists in the compulsory opening of access to the incumbent networks to all potential competitors, provided that they meet a certain number of established criteria. One version of this option envisages the structural separation, which the Commission foresees could in principle be imposed under competition law instruments. Until very recently, the most radical intervention of a regulatory authority in the commercial practice has been the institution of a compulsory licensing for dominant companies under Article 82 EC; that is, the essential facilities doctrine.

There are many advocates and critics of this regulatory measure, both in governmental and industrial circles. In the scholarly literature, there is a virtually consensus upon the fact that the essential facility doctrine constitutes the ultimate frontier of the regulatory interference into the 'societal sanctity' of the private property domain. The most radical version of this institute provides the possibility of compulsory opening access to a piece of private property, which constitutes an industrial bottleneck, but only under the principle of limited and shared access. It is almost impossible to imagine how the tools of *ex post* regulation may be used to impel the incumbents to refuse to operate on the market of communications services, leaving them merely the possibility of technically servicing the networks. The only possible way to implement this idea is through *ex ante* regulatory requirements, obliging member states to grant the NRA the necessary competences to guarantee that network operator

open access to all competitors by separating their infrastructure services from the provision of internet access. In all likelihood, the Commission considers this approach as merely theoretical and uses its argumentation for the purely methodological purposes of comprehension and analysis. For the sake of discussion, however, it is possible to simulate a situation similar to the famous rationale of the European courts with regard to parallel trading in intellectual property; namely, “the possession of property does not necessarily correspond to its usage, which might have been restricted”. By analogy, holding the network does not entail an unreserved right to provide electronic communications services. Hence, technically speaking, certain requirements of registration or establishing and accounting separation of the incumbents might be launched by the Commission.

The Commission is absolutely right in saying that the ‘open access’ model for new infrastructure investment works well in a *tabula rasa* situation, where there is no pre-existing network or Commission initiate proactive initiatives, using structural funds. This situation may be fully justified only under free-will but not under compulsory regulatory initiatives. The offered model has many advantages *per se*. Yet, because of the impossibility of separating the present-day infrastructure owners from the communications services, which often constitute the major part of their revenues, this idea remains mostly hypothetical.

The third option considered by the Commission is the absence of any change to the regulatory framework. The current model is characterised by a high degree of predictability and harmonisation and its capability to successfully regulate the European telecommunications area has been proved in practice. For this reason, it would be appropriate to concentrate efforts on the adaptation of the regulatory framework to rapid technological changes and direct them on the coverage of new-arising domains, rather than propose radical conceptual changes. The Commission considers that this model is the most appropriate option and has thus proposed it in its associated Communication.

### III. EUROPEAN AUDIOVISUAL POLICY

#### 1. *Network neutrality context*

In regulatory terms, the concept of network neutrality is in-between. Its substance relates equally to infrastructure and content. The fundamental essence of network neutrality is based upon the principle of fair treatment of content by network operators. Unlike traditional broadcasting, data over IP streaming has no technical borders and can potentially cover a worldwide audience. Since the issues of content management relating to

network neutrality may occur predominantly in the downstream market - namely, content destination, places of consumption of the content by customers-, the attention has to be paid to European regulatory instruments of content management.

Regulation of audiovisual contents represents a substantial segment of the European communications policy. The main legislative document in this area is the Directive on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities; "Television without Frontiers Directive" or TVWFD (89/552/EEC), from 1989. This document has been substantially updated in 1997. After some lengthy public debates and consultations, the Commission issued in 2005 and further amended in 2007 its proposal for Audiovisual Media Services Directive; AVMSD or Audiovisual Media Services Directive being a new title for TVWFD.<sup>6</sup>

The original objective of TVWFD is the creation of appropriate conditions for the free movement of television transmission within the EC. Its primary scope included all forms of public broadcasting, except electronic communications services providing information services on on-demand basis.

## 2. *Single European TV market*

In terms of the *liberation-integration-competition* paradigm, the main aim of this document has definitely been the second one. By opposition to the US context, the broadcasting industry in Europe is characterised by strong public elements. The state inheritance is either directly or at least implicitly present in all major European broadcasters and the whole consumer media culture in Europe. A genuine liberalisation of the broadcasting industry has never been on the European agenda. For this reason, TVWFD does not appear to concentrate any efforts on the liberalisation of the TV markets. Instead, it strives to integrate the different national regulatory environments into a single European model.

In order to pursue this important mission, the Commission tries to eliminate any regulatory borders between the different member states. Hence, one of the key ideas of the TVWFD has been the prohibition for the member states to conduct any measures, which can restrict reception or retransmission of broadcast signal from other member states, apart from public safety, the promotion of culture and similar exceptional

---

<sup>6</sup> Directive of the European Parliament and of the Council on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the provision of audiovisual media services.

national needs.

However, there are not enough political, economic and cultural preconditions for establishing a free market model for the TV industry in Europe. As is the case with the European regulation of the telecommunications infrastructure, the main efforts of the Commission are directed towards regulatory unification within the European internal market. The essence of *harmonisation* of the TV markets is based upon the subordination of national regulatory regimes to a pan-European one. Since the meta-task of European integration is based on the elimination of regulatory differences and economic borders between the member states, but by no means on erasing obstacles to an internal free market -as the internal market is not a free market-, the European audiovisual policy develops in parallel with the general objectives of the European integration. These regulatory roots of the European model of TV industry play a role in the present-day situation in relation to the production and distribution of European TV content. Without unnecessary oversimplifications, and fully taking into account all cultural, linguistic, behavioural and esthetical particularities of Europeans, there are enough evidences to conclude that there exists a direct relation between the strong regulatory character of the European TV industry and its poor commercial performance both in the world at large and the domestic markets.

TVWFD covers a broad range of issues, related to the production, transmission and reception of content in the EC. Its adoption has been originally stimulated by fast technological developments in the TV industry. In combination with the firm intention to establish a single European market, these prerequisites became decisive for the initiation of this legislative measure. Initially adopted in 1989, it has been amended in 1997 because of the further development of the audiovisual sector; in particular, in the area of satellite TV, marketing-oriented business models, interactive technologies and future deployment of cable infrastructure.

In 2007, EU is still revising TVWFD. Under the new title of Audiovisual Media Services Directive, it is called for providing an effective regulatory tool for content production and distribution in the new digital age.

Since the adoption of TVWFD in 1989 and its substantial amendment in 1997, electronic technologies have substantially expanded, leading the Commission to initiate in 2002 a legislative review of TVWFD. It has been officially launched by launching a proposal for the elaboration of a program for the modernisation of rules on audiovisual services and a timetable for future actions. The Commission organised an extensive public consultation campaign. As a result of this hearing, many research

and analytical programs and seminars have been organised by the Commission from 2003 until 2007. Finally, in 2005, the Commission officially adopted a legislative proposal for the revision of TVWFD, with some relevant amendments in 2007.

This document stresses the importance of the European audiovisual environment, based on principles of pluralism, cultural diversity and consumer protection. The Commission offers in this proposal to guarantee the independence of national regulators in the media sector; which essentially means to strive to provide the necessary tools for stronger regulatory powers.

#### IV. CONCLUSIONS AND OPENINGS FOR FURTHER RESEARCH

The aim of this contribution has been to give to a descriptive presentation of the current European regulatory framework in the areas of electronic communications and audiovisual policy. By analysing the relevant EC directives, it strived to put the existing model of *ex ante* regulation into the context of the network neutrality debates; with the general objective to provide a clear-cut overview of the European state of affairs in the areas related to network neutrality. The purpose of the overall project is not to present the mono-semantic meaning of this multidimensional problem, but rather to explore the nodular issues of the academic debates over network neutrality in the United States, to correct mistakes and afterwards to offer effective, theoretically adjusted solutions for the existing and new telecommunications operators in the European markets. The nature of argumentation is mainly legal and, to a lesser extent, economic or societal.

Departing from a conception favouring *ex post* regulation of network neutrality, one can demonstrate why exactly Europe does not deserve an explicit mention in the *ex ante* telecommunications framework. It goes without saying that any sort of instrumentalisation of explored arguments should be rejected and all pros and cons analysed without any partiality. This paper opens the path to the provision of an alternative approach to the network neutrality dilemma in the European context. One can expect *a priori* to give a positive answer to the question submitted in the title of the present proposal; that is, whether Europe should trust in antitrust.

From an academic perspective, network neutrality is an interdisciplinary phenomenon. It can be explored under its economic, legal, societal, technical and political dimensions. By applying political philosophy's argumentation and reasoning, one can attempt to prove that content *prioritisation* is, by far, not the same as content *discrimination*. In addition,

when exploring the existing US and EU case-law related to telecommunications, intellectual property and antitrust areas, one can provide economic, societal and (most importantly) legal argumentation for ISPs to content / application prioritisation and emphasise the relevancy of the *ex post* antitrust instruments for the companies which abuse or misuse their 'natural' right to prioritise the content.

The history of public debates in the United States showed a big potential for the network neutrality proponents to attract consumers. Their vivid rhetoric together with constant reference to fundamental freedoms manages to create a powerful public tool for the promotion of this idea. It is, therefore, important to explore and evaluate the most successful techniques, applied by the proponents of network neutrality. At this point, one can only foresee that the existence of extra-speed possibility for premium internet services is not likely to degrade the other applications and that higher data-speed option gives to consumers an opportunity to benefit from the great variety of internet services, particularly from those related to live-streaming. The rest is the object of a much wider project.

# **THE FUTURE OF LAW: RELATIONAL JUSTICE AND NEXT GENERATION OF WEB SERVICES**

Pompeu Casanovas\*

## **I. INTRODUCTION**

This paper deals with some hopes and some concerns about the future of law, which I believe specifically related to the future of the Internet and the next generation of Semantic Web services.<sup>1</sup>

I will contend three theses about the integration of knowledge, regulation and semantic technology that may shed some light on how the future of law and the Internet looks like:

- (1) There is a lack of scientific, reliable knowledge on how the Internet is really working and in which measurable way semantics is affecting development; so we would need a better integration of communication, social and computer technologies to run the web.
- (2) Usually, researchers in Artificial Intelligence and Law divide IT and Law into two different domains: (i) IT law —data protection, copyright, security, domain names...— and (ii) IT for lawyers —e-government, e-court, Online Dispute Resolution, Multi-Agent Systems...<sup>2</sup> Recent developments in semantic technologies, Natural Language Processing (NLP), legal ontologies, information retrieval technologies (IRT) and the Web 2.0 and 3.0 may contribute to the convergence of the two approaches into a single techno-legal one.

---

\* UAB Institute of Law and Technology (IDT), Autonomous University of Barcelona, Bellaterra.

<sup>1</sup> Marta Poblet and I wrote two more joint papers connected to this same subject. P. CASANOVAS, M. POBLET, “Adding Semantics to the legal Domain”, ESTC-08, Vienna, 2008; P. CASANOVAS, M. POBLET, “Justice via the Internet: Hopes and Challenges of Law and the Semantic Web”, 2009, P. CASANOVAS, M. POBLET, “Law Via de Internet”, ITTIG, Florence 30th October 2008.

<sup>2</sup> M. APISTOLA and A. LODDER, “Law Firms and IT. Towards Optimal Knowledge Management”, *Journal of Information, Law and Technology*, 2005, No 2/3, pp. 1-28. A. LODDER and A. OSKAMP, “Law, Information Technology and Artificial Intelligence” in: A. LODDER and A. OSKAMP Eds, “*Advanced Technology in the Legal Domain. From Challenges to Daily Routine*”, Dordrecht, Springer, 2006, pp. 1-22. M. LAURITSEN, “Artificial Intelligence in the Legal Real Workplace”, in: A. LODDER and A. OSKAMP Eds, “*Advanced Technology in the Legal Domain. From Challenges to Daily Routine*”, Dordrecht, Springer, 2006, pp. 165-176.

Second generation of Semantic Web technologies is one of the means to facilitate this convergence.

(3) Therefore, I think that a pragmatic and cognitive approach based on a better knowledge of legal users, scenarios and contexts may be helpful to develop SW applications and legal Web Services. I will call later *relational justice* this hybrid, mixed-up field, as a subset of *relational law* of contracts and *restorative justice* of crimes (private and public law).

I will rely on recent work and projects carried out by Internet scholars and by Semantic Web developers to foster a fruitful dialogue between AI & Law scholars and legal theorists. Nevertheless, in this paper, more technical issues such as knowledge representation, knowledge acquisition, legal ontology building and methodology will be put aside.<sup>3</sup>

#### 1. *What is happening with the Internet?*

Internet is growing every day. At the end of 2007, the Web had 1.3 billion users, and the growth rate in percentage for the period 2000-2007 was 920.2 % in the Middle East, and 882.7 % in Africa. Those are good news, even if we take into account the fact of the unequal distribution of resources and opportunities across the Web. However, in spite of its amazing growing, the old problem of gathering and representing content remains. How all the generated information flow may be retrieved, organized and shared in a feasible and reasonable way?

In a recent Conference on the Future of the Internet for the STI Assembly<sup>4</sup>, John Domingue<sup>5</sup> drew a broad landscape, in which a multitude of connected IT services are offered, bought, sold, used, repurposed, and composed by a worldwide network of service providers, consumers, aggregators, and brokers. This would result in a new way of offering, using, and organizing IT supported functionality, in which interoperability through Web 2.0, sensors, multi-media and what is called “The Internet of

<sup>3</sup> See the state of the art in legal ontologies in J. BREUKER, P. CASANOVAS, M. C. A. KLEIN, E. FRANCESCONI, “The Flood, the Channels and the Dykes: Managing Legal Information in a Globalized and Digital World”, in: J. BREUKER, P. CASANOVAS, M. C. A. KLEIN, E. FRANCESCONI (eds), *Legal Ontologies and the Semantic Web. Channelling the Legal Information Flood*, Amsterdam, IOS Press, 2009.

<sup>4</sup> ESTC, Vienna, September 26<sup>th</sup> 2008.

<sup>5</sup> V. R. BENJAMINS, J. DAVIES, R. BAEZA YATES, P. MIKA, H. ZARAGOZA, M. M. GREAVES, J.M. GÓMEZ-PÉREZ, J. CONTRERAS, J. DOMINGUE, D. FENSEL, “Near-term Prospects for Semantic Technologies”, IEEE Intelligent Systems, January/February 2008, pp.76-88.

Things” (and not only interconnected pages) would reach a great number of end users (government, companies, businessmen, employees, scientists, employees, consumers and citizens).

In this vision, Semantic Technologies would be the key for the Web 3.0. The term *Web 2.0* emerged from a 2004 brainstorming session among officials of O'Reilly Media, Inc., and MediaLive International.<sup>6</sup> The term *Web 3.0* was coined by John Markoff of the New York Times in 2006. Those terms may be seen as slippery concepts<sup>7</sup> or as shortcuts as well to refer to the interoperability and tagging allowing inputs from the users (Flickr, YouTube, Wikipedia, Facebook ...), and to adding semantics in more expressive languages to link objects and to share ontologies behind platforms and Web services.

As stated by many scholars, above all, the Web 2.0 is a *social network*, allowing people to connect each other and adding value through tagging to the websites that they populate with content. This content should be better organized through semantic technologies. This social pragmatic approach is all what SW is about.

Back to 2001, when the idea was spread out with an increasing strength, James Hendler envisaged a situation in which agents could easily construct ontologies to interoperate among them. An ontology-language (Hendler thought of *DARPA Agent Markup Language*, DAML + OIL) could be “easily” used to define ontology not of services but of the terms needed to describe the invocation of services. Using the example of a finite-state machine, this ontology would contain classes such as *State* and *Link* and have special Subclasses such *StartState* and *EndState*. Contents and properties could be described to give links a head and tail, to give states a list of the links that lead out from them, and to give a state an identifying property (Universal Resource Identifier).

Then, it would be easier to produce a domain ontology to perform social links. E.g. a “standard web sale” could be defined in some service ontology comprising a particular set of states and links.

The final result would be not only an intelligent human-interaction interface, but agent-to-agent communications that would produced social effects and perform social acts such as buying, selling and paying “between two Web agents that can use proof checking to confirm transactions”.

---

<sup>6</sup> D. E. HARMON, “The ‘New’ Web: Getting a Grip on the Slippery Concept of Web 2.0”, *Lawyer's PC*, 2006, vol. 23, n. 1, pp. 1-5.

<sup>7</sup> *Ibid.*

“An agent can send an annotated proof to other agent. The annotations can be pointers to a particular fact on the Web or to an ontology where a particular rule resides. The agent receiving this proof can analyze it, check the pointers and check that the ontology is one it can read and agree with. This lets the agents recognize that a valid transaction has occurred and allows the funds to be transferred.”

Hendler called this perspective “service logics”, and he predicted that this would be easy to achieve for the Web.

But nearly nine years later, this is still a hope, or an unfulfilled promise. *Where are all the agents?* is the title of one of his challenging letters from the editor for IEEE Intelligent Systems. After being involved in the creation of Darpa Agent Markup Language (DAML) and the Ontology Web Language (OWL), a standard since February 2004, Hendler recognizes that although there are enough ontologies, interoperability at the data level is being solved and the existence of open source toolkits, still, there are no intelligent-agent based systems operating in the web and no venture-capital really available (no business plan)<sup>8</sup>. So, “what happened”?

Putting aside the technical aspects, the answer may be related to the obstacles the Internet is facing today which are hindering a real science of the Web. This is again a matter of lack of knowledge. This may be a bit surprising, but the same social and economic networks that are fostering the growing of the Internet are actively becoming obstacles to the development of its full potential, and lawyers have some responsibility on that. This was anticipated, e.g. by Dan Hunter in 2003 when he warned IT lawyers about “the anti-commons paradox”: “we are enclosing cyberspace, and imposing private property conceptions upon it. As a result, we are creating digital anti-commons where sub-optimal uses of Internet resources are going to be the norm”.<sup>9</sup>

But let’s start with the explanations on social links among pages which constitutes the kernel of Web 2.0 before going into it.

The power of the web emerges through the link space realized between Web pages. This is known as *the network effect*. From the physical point of

---

<sup>8</sup> In the same sense, BENJAMINS et al., *supra* note 5: most SW applications deal with search, and only a few of them are deployed with corporate budgets.

<sup>9</sup> D. HUNTER, “Cyberspace as a Place and the Tragedy of Digital Anti-commons Paradox”, *California Law Review*, 2003, No 91, p. 439.

view (the first layer of the Internet), this is a *scale free network*.

The difference between a random and a scale-free network is the following<sup>10</sup>: (a) The random network is homogeneous: most nodes have approximately the same number of links; (b) The scale-free network is inhomogeneous: the majority of the nodes have one or two links, but a few nodes have a large number of links, guaranteeing that the system is fully connected.

At a large scale, many social phenomena show this kind of decreasing connectivity: fast development of diseases and epidemics, gossiping, city sizes or, even, the distribution of the human sexual contacts for males and females.<sup>11</sup> In the connectivity distribution  $P(k)$ ,  $k$  is the number of links connecting to a node. Scale free-networks are characterized by a power law decay of the cumulative distribution  $P(k) \sim k^{-\tau}$ , meaning that the probability of attaining a certain size  $t$  is proportional to  $k^{-\tau}$ . When  $\tau$  is greater than or equal to 1 we are under a Zipf law.<sup>12</sup> For the web, scale-free networks may be formed due to preferential attachment, i.e. new links are established preferentially between nodes with high connectivity. Therefore, “the rich do get richer”.<sup>13</sup>

The “network effect” has also come to be known as Metcalfe’s law. In the early 1980s Bob Metcalfe explained to his customers why they needed more Ethernet boards than they were buying, because while the cost of the network grew linearly with the number of connections, the value was proportional to the square of the number of users.<sup>14</sup>

However, it is worthwhile to keep in mind that all those reckonings, in a way, are hypothesis, *Gedanken experiments*. Researchers have come slowly to realize that we don’t know many things about the real size and functioning of the Internet, including the effects of adding semantics to the web. Hendler, Berners-Lee et al. have recently recognized this fact:

“Google receives more than 100 million queries per day, and if 20% of them are unique, then more than 20 million links, represented as

<sup>10</sup> JEONG, 2003.

<sup>11</sup> F. LIJEROS, C. R. EDLING, L. A. NEVES AMARAL, E. H. STANLEY, Y. ABERG, “The Web of Human Sexual Contacts”, *Nature*, 2001, No 411, pp. 907-908.

<sup>12</sup> L. A. ADA, B. A. HUBERMAN, “Zipf’s law and the Internet”, *Glottometrica*, 2002, No 3, pp. 143-150.

<sup>13</sup> F. LIJEROS et al., *o.c.*

<sup>14</sup> J. HENDLER, J. GOLBECK, “Metcalfe’s Law, Web 2.0 and the Semantic Web”, *Web Semantics: Science, Services and Agents on the World Wide Web*, 2008, Vol 6, No 1, February, pp. 14-20.

new URIs that encode the search term(s), should show up in the Web graph every day, or around 200 per second. Do these links follow the same power laws? Do the same growth models explain these behaviors? *We simply don't know.*"<sup>15</sup>

## 2. *Legal markets, ITC law and ITC for lawyers*

The though criticism that Kimberly Claffy, from the CAIDA San Diego Supercomputation Center, hold recently before the Stanford lawyers is entitled *Ten Things Lawyers should Know about the Internet*.<sup>16</sup> Many obstacles prevent good measurements both of the Internet and of the Web. Claffy summarizes in four points the main problems they encounter in mapping the web: (i) *security*: "the fundamentally insecure software ecosystem"; (ii) *scalability*: "the fundamentally unscalable routing and addressing architecture"; (iii) *sustainability*: "the fundamental unsustainable economic architecture"; (iv) *stewardship*: "a stewardship model broken along so many dimensions, that solving or even studying the first three points is no one responsibility."

The situation is this one.<sup>17</sup> National legislation sometimes does not help either, like in the case of the European ID cards.<sup>18</sup> However, I believe that

---

<sup>15</sup> J. HENDLER, N. SHADBOLT, W. HALL, T. BERNERS-LEE, D. WEITZNER, "Web science: An Interdisciplinary Approach to Understanding the Web", *Communications of the ACM*, July 2008, Vol 61, No 7, pp. 60-69.

<sup>16</sup> K. C. CLAFFY, "Ten Things Lawyers should Know about the Internet", 2008, [http://www.caida.org/publications/papers/2008/lawyers\\_top\\_ten/](http://www.caida.org/publications/papers/2008/lawyers_top_ten/) (accessed October 10th 2008).

<sup>17</sup> "Because no systemic measurements activities exist for collecting rigorous empirical Internet data, in many ways, we don't really know what the Internet actually is. Thus, we don't know the total amounts and patterns of data traffic, the Internet's growth rate, the extent and locations of congestion, patterns and distribution of ISP interconnectivity, and many other things that are critical if we're to understand what actually works in the Internet. These data are hidden because ISPs consider such information proprietary and worry that competitors could use it to steal customers or otherwise harm their business. The information might not even be collected because no economic incentive exists to do so, nor do any regulations require this collection." K.C. CLAFFY, S.D. MEINRATH, S.O. BRADNER, "The (un)Economic Internet?", *IEEE Internet Computing*, May-June 2007, pp. 53-58.

<sup>18</sup> "The result of legislation is that it has prevented the adoption of electronic identification instead of promoting it. The failure is evident by looking at what has been achieved so far. After 10 years of intense bureaucracy and tens of millions of Euros, we have not been able to implement a national eID scheme in Sweden. Even though there is a Swedish national ID card (INIDEL) capable of holding an electronic ID, it is empty. The card is essentially a brick! Essentially we are at the same point now as we were a decade ago. It is clear that something is fundamentally wrong." F. LJUNGRREN, "Complexity is the Achilles Heel of eID. The Swedish

professional behaviour under economic, political and cultural corporate constraints has much more to do with all of this.

In *Urban Lawyers*, Heinz and Nelson revisit their precedent study of 1982 on *Chicago Lawyers*.<sup>19</sup> Their insights are derived from a comparison of two surveys of the Chicago bar. The first was conducted with 777 lawyers in 1975 (when the profession was still numerically stable). The second was conducted on 787 Chicago lawyers in 1994 and early 1995. The authors show that the profession has experienced a dramatic change. For the first time, women, African Americans and Latinos have been involved in the profession, but in marginal roles in law firms and in lower-status practice settings. There is a growing divide between prestigious (corporate and tax law) and less-prestigious fields of law. A greater proportion of Chicago lawyers focus their work on corporate clients, get much more money and their economic values have become close to the business interests. Therefore, the profession has become more segmented and more conservative.

Brian Tamanaha (2006) conceptualized the emergent situation as a new “legal instrumentalism” opposed to a principled and more integer conception of the law that American lawyers had in the seventies and eighties.<sup>20</sup> Lawyers’ relentless competition, the billable hour’s system, and pressures to the partners to bring in clients have shaped new legal professional practices contrary to a vision of law as a matter of principle and reason. I am afraid he is right.

Some recent data may give some support to this statement, because the expansion of lawyering is related to an increasing use of ITC tools, as shown by the ABA surveys. In 2008, e.g., over 40% of the USA firms indicated an average \$ 8.000-\$ 17.000 spending per attorney. 72% of respondents report that the firm files court documents electronically, up from 55% in the 2007 survey.<sup>21</sup>

---

eID system”, *ENISA Quarterly Review. Security and Interoperability of eID*, 2008, Vol. 4 No. 3, pp. 16-18.

<sup>19</sup> J.P. HEINZ, R.L. NELSON, R.L. SANDEFUR, E.O. LAUMANN, *Urban Lawyers: The New Social Structure of the Bar*, Chicago, University of Chicago Press, 2005.

<sup>20</sup> B.Z. TAMANAHA, *Law as a Means to an End: Threat to the Rule of Law*, New York, Cambridge University Press, 2006.

<sup>21</sup> American Bar Association Technology Resource Center, *2008 ABA Legal Technology Survey Report: Online Research*, <http://meetings.abanet.org/ltrc/index.cfm?data=20080909> (accessed September 18th 2008).

Respondents are asked how they collaborate on documents. The methods reported most often are e-mail attachments (92%, up from 80% in the 2007 survey), fax (65%), Microsoft Word track changes or equivalent (64%), and in person (58%). Nearly all respondents report the ability to check work e-mail while away from the office (98%). The method reported most often by respondents as used to check e-mail while away from the office is via Smartphone/BlackBerry (59%).

According to the *The American Lawyer 100 Report* —the top-grossing law firms in the United States— total revenues reached \$ 64.6 billion and increased 13.6 % in 2007. At the top rank, two big firms, Skadden Arps Slate Meagher & Flom and Lathan & Watkins, reached more than 2 \$ billion (gross revenue) and 1.17 and 1.05 \$ million per lawyer. We may wonder whether such numbers are sustainable in the new economic landscape after the crisis of the Wall Street financial model. Lawyers themselves are starting to wonder whether such numbers are sustainable.<sup>22</sup> Some prudence is required before answering such a question.

However, those are not surprising news. Describing increasing legal revenues related to the so-called *big bang* of lawyers is a well-trodden path by economists, legal theorists and Law & Society researchers. Table 1 shows the reckoning of expected value from 2003 to 2008.

| Country     | Value in 2003    | Growth 2002-03 | Expected value in 2008 |
|-------------|------------------|----------------|------------------------|
| USA         | 140.3 billion \$ | 5.6 percent    | 174.1 billion \$       |
| UK          | 28               | 3.6            | 31.6                   |
| France      | 14.7             | 14             | 16.7                   |
| Australia   | 5.9              | 11.6           | 9.4                    |
| South Korea | 1.35             | -3.3           | 1.9                    |
| China       | 1.34             | 7              | 1.9                    |
| Japan       | 0.9              | 8              | 1.6                    |

Table 1. Legal markets size. Source: Euromonitor.

What is new is the convergence between lawyering and technical knowledge either of the Internet or the World Wide Web (WWW).<sup>23</sup>

<sup>22</sup> A. PRESS, J. O'CONNOR, "Lessons of the Am Law 100: Is the Golden Age Over?", *The American Lawyer*, 05/01/2008.

<sup>23</sup> M. POBLET, P. CASANOVAS and V.R. BENJAMINS, "Technology and Law: The Not So Odd Couple", in: P. WARREN, J. DAVIES and D. BROWN (Eds), *ICT Futures. Delivering Pervasive, Real-time and Secure Services*, Chichester, John Wiley & Sons Ltd, 2008, , pp. 201-211. J. BREUKER *et al.*, *supra* note 3.

Practicing law becomes easier as long as legal operators use electronic devices to perform their jobs. Of course, we may take into account that size makes a big difference between soloists and corporate lawyers. But, still, ICT for lawyers is an emerging flourishing field both for small and big companies. Law firms may diverge in the toolkits they use and seek for, but not in the fact that their daily work rely increasingly on the use of technology. Semantic technology is being developed in the law field according to these needs.

Collaborative tools (extranets, *blawgs*, wikis..) and meta-data use (watermarking documents, digital times stamping, *clickwrap* agreements...) are being commonly adopted, especially by young lawyers. Less attention is paid for the moment to XML technologies and legal multimedia trends (beyond videoconferences).

But perhaps the best example of how ICT law and ICT for lawyers are related and will be even more related in the next future is the e-Discovery development.

E-Discovery is experiencing a spectacular growth because of the nature of the legal process itself. Electronic Data Discovery (EDD, or e-Discovery) may be defined as “a process (or series of processes) in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case, or as part of a court-ordered or government sanctioned inspection”.<sup>24</sup> Electronic Stored Information (ESI) is difficult to recover and retrieve because of its massive character. It is usually saved on back up tapes that are not labeled, catalogued or organized properly. Indexing and tagging requires both legal knowledge and computer expertise.

Moreover, as Will Uppington has noticed, EDD is a field in which it becomes necessary to combine concept and keyword search with content categorization technologies.<sup>25</sup> Therefore, there is room enough for a

---

<sup>24</sup> S. ATTFIELD, A. BLANFORD, *E-discovery viewed as integrated human-computer sensemaking: The challenge of 'frames'*, 2008, <http://eprints.ucl.ac.uk/9135/1/9135.pdf> (accessed August, 31st, 2008)

<sup>25</sup> “Surely, concept search technology is better than old, boring keyword search. Well, actually it’s not that clear-cut. The problem with concept search technology is that while it might find more relevant documents than plain keyword search, it will also likely find more false positives. Imagine searching for documents containing “terminate” in an employment matter and your concept search technology automatically searching for “fire”, “dismiss”, etc. as well. You’ll find more documents related to the termination of employees, but you’ll also find a lot more non-relevant documents concerning house fires, the fire department, etc. So concept search can

plurality of approaches, which lie on the different purposes and aims of users.

End users —customers, citizens, rulers, administrators...— and not only law firms or tech companies are real players in the field as well, because eventually someone has to pay the high costs of e-Discovery programs, as players have become to understand.<sup>26</sup>

### 3. *Web Services and Second Semantic Web generation*

The main objectives of next generation of the Semantic Web are related to this plural and hybrid approach. What conception of law may be figured out to comply with them? I will link the two issues in my answer in the next two sections.

Comparing first and second generation of Semantic Web applications, E. Motta and M. Sabou identify several features of the new orientations: (i) reuse (vs. semantic data generation); (ii) multi-ontology systems (vs. single-ontology systems); (iii) openness with respect top semantic resources, (iv) scale as important as data quality, (v) openness with respect to Web (non-semantic resources), (vi) compliance with the Web 2.0 paradigm, (vi) openness to services.<sup>27</sup>

Personalization, user-centered approaches, semantic wikis, hybrid ontological solutions, synergies between folksonomies and ontologies, scalability and meta tagging of great amounts of web-stored available data,

---

help address the under-inclusive problem with keyword search, (though it won't solve it) and can be helpful during analysis. But it can often increase the over-inclusive problem." W. UPPINGTON, *Concept Search Versus Keyword Search in Electronic Discovery*, 2008 <http://www.clearwellsystems.com/e-discovery-blog/2008/11/12/concept-search-versus-keyword-search-in-electronic-discovery/> (accessed January 15th 2009).

<sup>26</sup> "[Hewlett-Packard] says using lawyers to search through 100 gigabytes of data would cost about \$ 180.000. But since its software automatically culls irrelevant documents, attorneys in such a case would have to go through only a small portion of that data —for a cost of about \$ 25.000. [...] Recently, tech companies and lawyers have taken steps to solve their conflict. Some law firms that handle big business cases —such as Fenwickand San Francisco's Howard, Rice, Nemerowski, Canady, Falk & Rabkin, among others— now consult with clients on which e-Discovery software to choose and how to use it". J. SCHECK, "Tech Firms Pitch Tools for Sifting Legal Records", *Wall Street Journal*, 22 August 2008.

<sup>27</sup> E. MOTTA and M. SABOU, "Next Generation Semantic Web Applications", in: R. MIZOGUCHI, Z. SHI AND F. GIUNCHIGLIA (Eds), [ASWC 2006], "The Semantic Web", LNCS 4185, Heidelberg and Berlin, Springer, 2006, pp. 24-29.

and web-services orientation seem to be the next step.<sup>28</sup>

Especially Dieter Fensel envisages the future of the SW as a “Web of services” in which “scalable interoperability not only requires semantics, but it cannot even be imagined without the usage of semantics”.<sup>29</sup>

In 2004, Fensel and Bussler provided a fully-fledged framework —Web Modeling Service Framework (WMSF)— to provide a conceptual model to develop services according to the principle of maximal decoupling complemented by a scalable mediation service: (i) strong decoupling of the various components that realize an e-commerce application; (ii) strong mediation service enabling anybody to speak with everybody in a scalable manner.

Web Services connect computers and devices with each other using the Internet to exchange data and combine data in new ways. They may be defined as software objects that can be assembled over the Internet using standard protocols to perform functions or execute business processes. It seems to me that Fensel and Bussler’s dynamic framework does not translate Hendler’s original idea of “services logic”, but goes in the same direction.

In contrast, many experienced researchers —mainly from Yahoo— recall that information retrieval is still one of the main functionalities of the Web. Bridging SW and information retrieval technologies faces scientific problems on knowledge representation and natural language understanding that remain still unsolved. The Semantic Web would fail to achieve the impact envisioned a decade ago on search on the World Wide Web. The question is this one: Why has the Semantic Web had so little effect on search services?

“We put forward three possible reasons. First, this integration is an

---

<sup>28</sup> V. R. BENJAMINS *et al*, *supra* note 5. J. DAVIES, M. GROBELDNIK, D. MLADENIĆ, “Challenges of Semantic Knowledge Management”, in J. DAVIES, M. GROBELDNIK, D. MLADENIĆ (Eds), *Semantic Knowledge Management. Integrating Ontology Management, Knowledge Discovery, and Human Language Technology*, Heidelberg and Berlin, Springer Verlag, 2008, pp. 248-251. P. WARREN, J. DAVIES and D. BROWN, “Conclusions”, in: P. WARREN, J. DAVIES and D. BROWN (Eds), *ICT Futures. Delivering Pervasive, Real-time and Secure Services*, Chichester, John Wiley, 2008, pp. 229-233. D. FENSEL, *STI Technical Report 2008-01-10*, STI Innsbruck, 2008, <http://www.sti-innsbruck.at/fileadmin/documents/SemanticTechnology.pdf>.

<sup>29</sup> *Supra* note 28. D. FENSEL and C. BUSSLER, *The Web services Modeling Framework (WSMF)*, 2004.

extremely hard scientific problem. Second, the Web imposes hard scalability and performance restrictions. Third, there's a cultural divide between the Semantic Web and Information Retrieval disciplines.”<sup>30</sup>

This is true, and I am not discussing it. But *hybrid* theoretical approaches and more pragmatic perspectives are possible as well. In other words, it is not necessary to carry out first a complete fundamental research on the web to develop toolkits and strategies. Knowledge and the Internet in a whole are growing faster than that, stemming from practice and competition among technology companies and research institutes. We learn and we develop and test new languages, applications and theories with the same blow. Relying on this experience, a sharp distinction between fundamental and applied research does not make a lot of sense in this domain. The science of the Internet may combine many different approaches at the same time.

This has been noticed, again, by Jim Hendler when describing how Web 2.0 and web 3.0 are technically related. Table 2 shows the way Web 3.0 extends current Web 2.0 applications using Semantic Web technologies and graph-based, open data.<sup>31</sup>

|         |                           |
|---------|---------------------------|
| Web 3.0 |                           |
| Web 2.0 | Semantic Web (RDFS, OWL)  |
|         | Linked Data (RDF, SPARQL) |

Fig. 2 Source: Jim Hendler (2009)

We may bear in mind, as shown by the *Gartner Hype Cycle for Legal and*

<sup>30</sup> R. BAEZA-YATES, P. MIKA and H. ZARAGOZA, “Search, Web 2.0, and the Semantic Web”, in: V.R. BENJAMINS (Ed), *Near-term Prospects for Semantic Technologies, IEEE Intelligent Systems*, January/February, 2008, pp. 80-82.

<sup>31</sup> “RDF Schema (RDFS) and the Web Ontology Language (OWL) provide the ability to infer relationships between data in different applications or in different parts of the same application. These Semantic Web languages allow for the assertion of relationships between data elements, which developers can use, via custom code or an emerging toolset, to enhance the URI-based direct merging of data into a single RDF store”. J.HENDLER, “Web 3.0 emerging”, *IEEE Intelligent Systems*, January 2009, p.89 (pp. 88-90).

*Regulatory Information Governance* (16 July 2007) that SW is not a completely mature technology, at least not yet.

A Hype Cycle is a “graphic representation of the maturity, adoption and business application of specific technologies”. Since 1995, Gartner has used Hype Cycles to characterize the over-enthusiasm (*hype*) and subsequent disappointment that typically happens with the introduction of new technologies. Hype Cycles also show how and when technologies overcome the hype, achieve practical benefits, and become eventually accepted. This may happen now with Semantic Technologies.

However, there are more reasons of theoretical nature to explain the actual development of the SW towards a combination of top-down, bottom-up and middle-out strategies. It has been repeated many times in the literature that the Semantic Web should not be confused with Artificial Intelligent techniques. AI is about engineering. On the other side, the SW is a “web of data”: “a technological infrastructure to enable large scale data interoperability”.<sup>32</sup> In this sense, the SW has to be combined with other artificial devices to be effective. Adding semantics to the web, alone, does not solve either classical AI problems or satisfy users’ needs and demands.

This is especially true in the law field, because in spite of the already many available ontologies, very few applications have been built up following SW specifications. Law is not one of the main domains in which SW developments have been applied.<sup>33</sup> Ontologies are hard to build and especially to maintain. Martin Hepp talks about the *expressivity-community size frontier*: “the more detailed and expressive the ontology, the smaller the actual user community will be because it increases the resources necessary for reviewing and understanding the specification and associated documentation, which makes committing to the ontology reasonable only for a smaller number of individuals”.<sup>34</sup>

If SW is not only a web of information, but a web of knowledge, then the

---

<sup>32</sup> M. D’AQUIN, E. MOTTA, M. SABOU, S. ANGELETOU, L. GRIDINOC, V. LOPEZ and D. GUIDI, “Toward a New Generation of Semantic Web Applications”, *IEEE Intelligent Systems*, May/June 2008, pp. 20-28.

<sup>33</sup> Law is not even mentioned in survey on the subject by J. CARDOSO, “The Semantic Web Vision: Where We Are?”, *IEEE Intelligent Systems*, September/October 2007, pp. 84-88. According to him, education, computer software, government, business services and life sciences are the main domains of SW applications.

<sup>34</sup> M. HEPP, “Possible Ontologies. How Reality Constraints the Development of Relevant Ontologies”, *IEEE Intelligent Systems*, January/February 2007, pp. 90-96.

*nature* of knowledge to be modeled does matter as well. In the SEKT project<sup>35</sup>, we defined legal knowledge as being practical, dynamic and changing according to the community that is producing and using it. There is a lay knowledge of law, and a *professional legal knowledge* (PLK) which is shared across members of a legal social group (lawyers, attorneys, judges, prosecutors...) having in common their experience and practical knowledge of the law (Casanovas et al. 2004, 2005). These features facilitate the building of *ontologies of professional legal knowledge* (OPLK).

However, this leads to a kind of paradox, because assembling, classifying, sharing and reusing experiences are different and not necessarily coordinated and consistent tasks. Consistency between sharing and reusing cannot be taken into account. Some strategy is explicitly required if the object to be modeled is *experience* or *practical knowledge*, as Enric Plaza (2008) is pointing out in the so-called EDIR cycle (Express, Discovery, Interpret, Reuse). This is still an open discussion.

#### 4. *Relational Law and Relational Justice*

Let's go into the *experiences of law* now. Law, and not only the web, is changing fast too. Traditional fields of legal drafting, private contracting, judicial sentencing and administrative management have been enlarged with all the Online Dispute Resolution (ODR) initiatives and new forms of self-regulation and access to justice. In sharp contrast to corporate law practices, the web fosters new *personal* strategies. Citizens —as individual persons as much as citizens belonging to a political body— require a greater participation and faster and more effective ways of facing their legal activities. Dialogue, flexibility and autonomy seem to be the aim of new legal forms of *relational administration* and *relational justice*.<sup>36</sup>

Originally, we coined this concept for the sake of Restorative Justice, in a broad sense. *Relational Justice* (RJ) was defined as a bottom-up justice, the justice produced through cooperative behavior, agreement, negotiation, or dialogue among actors in a post-conflict situation (the aftermath of private

<sup>35</sup> P. CASANOVAS, M. POBLET, N. CASELLAS, J-J VALLBÉ, F. RAMOS, V. R. BENJAMINS, M. BLÁZQUEZ, J. CONTRERAS, J. GORROÑOGOITIA, D10.2.1.Legal Scenario, OPL Ontology and Architecture. EU-IST Project IST-2003-506826, SEKT (Semantically Enabled Knowledge Technologies), Deliverable Programa IST. 191 pp. <http://www.sektproject.com/rd/deliverables/wp10/sekt-d-10-2-LegalScenario.pdf/view>.

<sup>36</sup> P. CASANOVAS and M. POBLET, "Concepts and Fields of Relational Justice", in: P. CASANOVAS, G. SARTOR, N. CASELLAS, R. RUBINO (eds), *Computable Models of the Law: Languages, Dialogue, Games, Ontologies*, LNAI 4884, Berlin and Heidelberg, Springer Verlag, 2008, pp. 323-339.

or public, tacit or explicit, peaceful or violent conflicts) (Casanovas and Poblet, 2007, 2008).<sup>37</sup> The RJ field included ADR and ODR, mediation, commercial, labor and economic mediation, victim-offender mediation (VOM), restorative justice (dialogue justice in criminal issues, for juvenile or adults), transitional justice (negotiated justice in the aftermath of violent conflicts in fragile, collapsed or failed states), community justice, family conferencing, and peace processes.

However, recent developments of the Internet and recent trends in the Semantic Web area have convinced us to expand and change this definition in a more framed and regulatory way. *Relational Justice* may be defined as the substantive and formal structure that allows end users, in the broader sense (as citizens, consumers, customers, clients, managers, officials...), to participate in the making of their own regulation and legal outcomes through all the mixed and plural strategies that the Semantic Web framework allows. This implies the coexistence of legal and social norms, rights and duties to be shared by subjects (artificial or natural agents) in a structured environment. Therefore, user centered strategies of the next SW generation fit into a middle-out legal approach in which there are rights to be protected and duties to be put in place. The expressive content of Web 2.0 may be shaped as well by the service-oriented motivation of the Web 3.0.

From a more traditional point of view, relational justice may be described as a subset of *relational law*. This is not a new concept, either in public or private law. Regulatory bonds through the emergence of a shared context are the base of several sociological descriptions<sup>38</sup> and well-known classifications of contracts —e.g. the notion of *relational exchange norms*.<sup>39</sup>

On the other side, global justice and governance have been described many times as *relational*, to emphasize the contrast with public law theories based on the abstraction of a social contract to found some kind of sovereignty. For some criminologists, relational justice is a perspective to bear upon the problems raised by the criminal justice system: “to regard crime primarily as a breakdown in relationships; even in those cases where the offender does not know the victim, a relationship can be said to exist

---

<sup>37</sup> *Ibid.*, P. CASANOVAS and M. POBLET, “Micro-foundations of Restorative Justice”, in: R. MACKAY, Ch. PELIKAN, J. DECLERCK, B. v. STOKKOM (eds), *Images of Restorative Justice Theory*, Frankfurt, Ed. Polizei und Wissenschaft, 2007, pp. 235-256.

<sup>38</sup> S. MACAULAY, “Non-contractual relations in business: a preliminary study”, *American Sociological Review*, 1963, No 28, pp. 55-67.

<sup>39</sup> I. R. MACNEIL, “Relational Contract: What We Do and Do Not Know”, *Wisconsin Law Review*, 1985, No 3, pp. 483-525.

by virtue of their being citizens together, bound together by rules governing social behavior”.<sup>40</sup>

Legal theorists with a high degree of commitment with the Restorative Justice movement use to emphasize the role of privileged actors to counter-balance power in the political arena. For instance, in their thorough and well-known book *Global Business Regulation* (2000), John Braithwaite and Peter Drakos state at the end: “Our conclusion is that NGOs are the key to invigorating global good governance”.

Nevertheless, we think that Web 2.0 and Web 3.0 are beyond political activism, and this perspective may not be easily captured under private or public law either. The magnitude of relational bonds and trends becomes evident once we show the numbers. It is worthwhile to quote here explicitly a forthcoming paper by Colin Rule<sup>41</sup>, from e-Bay:

“If you have any doubt that consumers are moving to online commerce, take a look at eBay, the online auction company. In the 13 years since it was founded, eBay has grown into the largest marketplace in the world. In the first half of 2008, there were more than one billion product listings added to eBay worldwide. At any given moment, there are more than 100 million listings around the world, and approximately 7.1 million listings are added each day. eBay users trade almost every kind of item imaginable, in more than 50,000 categories. On eBay, a pair of shoes sells every 7 seconds, a cell phone sells every 7 seconds, and a car sells every 56 seconds. The daily volume of trade on eBay is greater than the daily volume of the NASDAQ.

Unsurprisingly, all of these transactions generate a lot of consumer disputes. Even though less than 1 percent of purchases generate a problem, the incredible volume on the site means eBay handles more than 40 million disputes a year, in more than 16 different languages”.

It has been highlighted the *democratic* model that the Web 2.0 implies. People can cooperate and build up in common their ideas.<sup>42</sup> Enriching this process seems a quite natural move from the Semantic Web perspective. But this is not an easy task.

---

<sup>40</sup> M. SCHLUTER, “What is Relational Justice?”, in: J. BURNSIDE and N. BAKER (eds), *Relational Justice: Repairing the Breach*, Winchester, Waterside Press, 1994.

<sup>41</sup> C. RULE, “Making Peace on eBay: Resolving Disputes in the World’s Largest Marketplace”, *ACResolution Magazine*, Fall 2008. I thank Colin for allowing me to quote his still unpublished paper.

<sup>42</sup> E. MOTTA, “Knowledge Publishing and Access on the Semantic Web: A Sociotechnological Analysis”, *IEEE Intelligent Systems*, May/June 2006, pp. 88-90.

Web services, collective work (Petrie 2008) and, lately, service parks (Petrie and Bussler 2008) constitute the natural path leading from Web 2.0 to Web 3.0 too. However, this means accepting that what Charles Petrie calls *the Academic Web Services Dream*, “a dream of an open and free Internet that could offer everyone a nearly infinite choice of services and ways to combine them” is changing as well. Big players count and are able to offer more flexible and friendly user services to a kind of customer seeking for brand and simplicity. Sets of services come with their own set of rules, adding complexity to the managing of the service and the interface with users. From a legal point of view, managing conflicts are as important as managing transactions, and copyright and copyleft are coexisting and overlapping in the web.

Those are some of the reasons why we chose as a research strategy building up legal platforms, easily accessible, and cooperating into the development of electronic agents able to negotiate, to reach agreements and help in regulatory tasks.

As Kalfoglou et al. (2004) noticed at the beginning of this process, “the increasing use of Web services to express computation on the SW points to a purely procedural notion of agency, while the kinds of reasoning which are envisaged in the description of the SW appear to require something more complex, e.g. proactive behavior”.

Agency, trust, dialogue protocols, dialogue games and social policy require a cooperative effort coming from lawyers, legal theorists and computer scientists. Some of the new trends have to concentrate on well-known areas with unsolved problems (such as information retrieval); some of them point to the same direction as SW developments (as Web services do); some of them face genuinely new challenges that anticipate the cognitive behavior of users in the web (as legal multimedia, imaging and the building of multimedia ontologies introduce). But *all of them* require a fast change of perspective in favor of interdisciplinary knowledge and cooperative work at theoretical level.

Moreover, computation is increasingly applied to solve or at least to manage social and regulatory problems than in the past where led to the only application or enforcement of law. Security and immigration are privileged fields in EU and USA. Business and corporate governance is another organizational field in which regulation is reached through a combination of principles, protocols, legal rules, ontologies and automatic (or semiautomatic) computation of internal logs. Thus, not only law, legal concepts and reasoning may be conceived and explained as a *cognitive*

*technology*<sup>43</sup>, but the social situated knowledge that enables law to be created, implemented and shared in an increasingly technological social and organizational environment.

#### **ACKNOWLEDGEMENTS**

NEURONA TSI-020100-2008-134; ONTOMEDIA CSO2008-05536/  
SOCI, TSI-020501-2008-131; INTEGRA.

---

<sup>43</sup> G. SARTOR, *Legal Reasoning: A Cognitive Approach to the Law. Vol. 5. Treatise on Legal Philosophy and General Jurisprudence*, Berlin, Springer, 2005

# **THE OPEN REVOLUTION: USING CITATION ANALYSIS TO IMPROVE LEGAL TEXT RETRIEVAL**

Anton Geist<sup>\*</sup>

## **I. INTRODUCTION**

The legal discipline is an unusually information-rich one. Contrary to other disciplines, there is not only an enormous mass of texts about the law, but also the law itself is textual in nature.<sup>1</sup>

Consequently, being able to automatically retrieve texts from large document collections was one of the first applications of computer science in the field of law.<sup>2</sup>

Today, when legal professionals log onto online databases of legal service providers in order to retrieve the text of court cases, statutory material or other legal documents, the process of obtaining those documents is called legal text retrieval. Put simply, legal text retrieval systems like Westlaw (United States, United Kingdom), LexisNexis (United States, United Kingdom and other countries), Beck-Online (Germany) and RDB (Austria) provide electronic access to legal documents and enable users to search within their text collections.

Citation analysis looks at citations to and from documents. The theoretical foundation on which the indexing of citations is built upon, is as follows: if there is a citation between two documents, there is some kind of relationship between these texts.<sup>3</sup> This relationship can be further explored and used to learn more about the characteristics of the connected documents.

Citation analysis of World Wide Web documents enabled the Internet search engine Google to outperform all other Web search engines that did not yet make use of the citation structure of the Web. Google decides on the relevance of Web pages to users' queries not only because of the text

---

<sup>\*</sup> University of Edinburgh, United Kingdom

<sup>1</sup> R. WIDDISON, "New Perspectives in Legal Information Retrieval", *Int J Law Info Tech*, 10(1), 2002, pp. 41-70, at p. 4.

<sup>2</sup> M.-F. MOENS, "Innovative techniques for legal text retrieval", *Artificial Intelligence and Law*, 9(1), 2001, pp. 29-57, at p. 29.

<sup>3</sup> J. FEATHER & R.P. STURGES, *International encyclopedia of information and library science* (2. ed), London: Routledge, 2003, at p. 76.

of those Web pages, but also because of their link structure. So far, no similar technological change has occurred in the area of legal text retrieval.

## II. LEGAL TEXT RETRIEVAL SYSTEMS TODAY

When we take a closer look at the legal text retrieval systems just mentioned, it is worth trying to put their use in a wider perspective.

The global market for legal text retrieval is big, with revenues of about EUR 3 billion per year to a vast number of online services around the world.<sup>4</sup>

After some experimental work, both in the USA and in Europe, the first legal text retrieval systems were implemented in the 1970s. Today it would be difficult to imagine the practise of law without the use of online legal databases, be it to retrieve legislative texts, court cases or legal literature. Distributed computing made it possible for lawyers to perform so-called computer-assisted legal research tasks from their own desks, rather than from a shared terminal.<sup>5</sup>

When commercial legal search engines were introduced, they were custom-built, often proprietary, software. Professional legal users have been expected to undergo some kind of special training in order to effectively use the specific legal databases.<sup>6</sup>

Technologically speaking, legal database providers around the world generally still use the same search technologies that they did when the databases were built. Those technologies, that belong to the "extended Boolean model", require the users to formulate strict queries, using so called Boolean operators (AND, NOT, OR, and others) to tie together individual words or phrases that form the search query.<sup>7</sup>

A characteristic of Boolean retrieval models is their "exact match" nature. They do not take into account any partial matches of queries. The search

---

<sup>4</sup> L. KLASÉN, "Legal IR services - from past to present", In C. Magnusson Sjöberg (Ed.), *Legal Management of Information Systems - incorporating law in e-solutions*, Lund: Studentlitteratur, 2005, pp. 337-358, at p. 338.

<sup>5</sup> C. TAPPER, "Out of the box", *International Review of Law, Computers & Technology*, 19(1), 2005, pp. 5-11, at p. 8.

<sup>6</sup> P. JACKSON & I. MOULINIER, *Natural language processing for online applications: Text retrieval, extraction and categorization* (2nd rev. ed., Vol. 5), Amsterdam Philadelphia: John Benjamins Pub, 2007, at pp. 64-65.

<sup>7</sup> C.D. MANNING, P. RAGHAVAN & H. SCHÜTZE, *Introduction to information retrieval*. New York: Cambridge University Press, 2008, at pp. 14-15.

engine will return results that fulfil all the criteria defined by the query, and only those. If a document fulfills all but one requirement, it will still not be returned as a result. Besides that, (extended) Boolean retrieval models do not employ any sophisticated technologies to rank the listed results.

Consequently, legal database providers still (have to) provide special training for their users outlining the peculiarities of Boolean syntax, proximity operators and field searching.

The main legal database providers have not ignored all technological advances in search technology in the past decades. It appears, however, as if both providers and customers have somehow agreed on settling for search technology that would be considered to be dated in most other disciplines.

Let us look at the example of Westlaw: The database provider is the largest commercial legal search service in terms of the number of paying subscribers. Over half a million subscribers perform millions of searches a day over tens of terabytes of text data.<sup>8</sup>

Today, Boolean search (called “Terms and Connectors” by Westlaw) is still the default search mode on Westlaw, and used by a large percentage of users. A technologically more advanced ranked retrieval search mode (called “Natural Language” by Westlaw) is available, but most users prefer the Boolean search.<sup>9</sup>

One is tempted to think that the legal material is simply not suited for more advanced search technologies. If the described Boolean legal text retrieval systems were performing well as legal research tools, there would really be nothing wrong with legal text retrieval using long established search methods. Ironically, however, the deficiencies of Boolean legal text retrieval have been known for decades.

The so-called STAIRS study conducted by Blair and Maron in the mid-1980s was the first legal retrieval experiment in a realistic operational environment. The searchers had a predefined goal to work on their queries until they were confident that the search had retrieved at least 75 percent of the total number of relevant documents. Further investigation, however,

---

<sup>8</sup> C.D. MANNING, P. RAGHAVAN & H. SCHÜTZE, *Introduction to information retrieval*, at pp. 14-15.

<sup>9</sup> P. JACKSON & I. MOULINIER, *Natural language processing for online applications*, at p. 28.

proved that while the result lists did not include a lot of off-topic results ("precision" was 79 percent), the average "recall" achieved by the Boolean system was no better than 20 percent. In other words: When the searchers thought that they had built a query that would give them 75 percent of all the relevant documents, the text retrieval system was only able to locate as little as 20 percent of those relevant documents.<sup>10</sup>

Although the Blair and Maron study has been triggering a passionate debate on the effectiveness of Boolean information retrieval systems in large full-text databases, legal text retrieval systems still build upon the same search technology that they did in the mid-1980s.

### III. THE NEED FOR BETTER LEGAL TEXT RETRIEVAL

A thorough discussion of why both providers and customers of legal text retrieval systems have (implicitly) accepted using dated search technologies is far too complex to be dealt with within this paper. A mix of several characteristics seems to be responsible for this. Let me just mention one of the major reasons for this fact. It not only explains why people do not use more up-to-date technology in the legal domain, but also shows very clearly why this situation must be changed.

Attorneys have the legal obligation to provide competent representation to their clients. In the U.S., but also in Europe, it has long been decided that the ability to perform adequate legal research is a component of this legal obligation. If an attorney fails to perform competent research, this constitutes a violation of their ethical duty and has led to malpractice suits against negligent lawyers.

As new computerised research tools have become available to lawyers, the standard of competence for attorneys concerning what "adequate legal research" means has arguably been increased.<sup>11</sup>

This puts the providers of legal text retrieval systems in a difficult situation: They want to provide their customers with electronic research tools, but at the same time they are eager to make sure that (sued) attorneys cannot argue that it was not them, but the search engine that failed to do "adequate legal research". The situation of the systems' users,

---

<sup>10</sup> D.C. BLAIR & M.E. MARON, "An evaluation of retrieval effectiveness for a full-text document-retrieval system", *Commun. ACM*, 28(3), 1985, pp. 289-299.

<sup>11</sup> M. WHITEMAN, "The Impact of the Internet and Other Electronic Sources on an Attorney's Duty of Competence Under the Rules of Professional Conduct", *Albany Law Journal of Science and Technology*, 11, 2000-2001, pp. 89-103, at p. 90.

on the other hand, is quite special too: They are certainly interested in tools that facilitate their legal research, but at the same time they want to avoid any increase in their standard of competence. A silent agreement that old search technology is "good enough" seems to be a plausible solution for both parties.

As soon as we remind ourselves that it is really not only the two mentioned parties who have to deal with the effects of more or less advanced search technology, it becomes obvious why it is in fact a necessity to use the most sophisticated search tools available. Legal documents build the foundation of every legal system. Better retrieval of legal texts effectively improves the work of all legal professionals, be it the judiciary, lawyers or legal researchers. This improvement, in turn, is useful for everyone who is affected by the legal system, which is society as a whole.

#### **IV. IMPORTANCE OF CITATIONS FOR LEGAL RESEARCH**

For a long time lawyers have consequently developed very sophisticated forms of citation handling. One just has to think of the various manuals of legal citations that are published, contrary to other disciplines. Part of the reason for the great importance of citations in legal texts lies in the nature of legal texts themselves. There is no physical "legal object" that is described in texts, the texts themselves constitute the law.<sup>12</sup>

When judges write opinions, they perpetually cite cases and other authorities. Legal scholars write articles and treatises that cite cases and other authorities, and which in turn are, at least sometimes, cited by cases and other authorities. These citations hold a great amount of information in them. Judges cite those cases that they think are the most relevant ones to the case they are deciding. Therefore, when two judges who are deciding different cases, cite some of the same authorities, this does mean that those cases are, at least somehow, relevant to each other.<sup>13</sup>

In common law countries, because of the eminent importance that citations play in those legal systems, there are specific tools and services that aim to assist attorneys in citation research. So-called Citator services allow users to see all citations that directly refer to a given case. Globally, the two biggest Citator services are LexisNexis's Shepard's, and WestLaw's

---

<sup>12</sup> C. TAPPER, "Citation Patterns in Legal Information Retrieval", at p. 258.

<sup>13</sup> T.A. SMITH, "The Web of Law", *The San Diego Law Review*, 44, 2007, pp. 309-354, at p. 341.

KeyCite.<sup>14</sup>

But citators not only allow researchers to verify the authority of a precedent by listing subsequent sources that have cited a source. They are also used by legal professionals to find additional sources relating to a given subject, by using the compiled citations as references to (somehow) related material.

Online legal databases certainly do provide access to citator services online, but given the enormous practical use of citators, it seems strange that they do not make use of legal citations to improve their (keyword) search results. So far, the result lists of legal text retrieval systems like Westlaw or LexisNexis are based solely on word occurrences, not on citations between legal documents.

## V. USING CITATIONS FOR LEGAL TEXT RETRIEVAL

Taking into account the importance of citations in legal research and the deficiencies of current legal text retrieval systems, it appears to be just a question of time that legal databases will have to make use of citation analysis of their document collection to improve their search results. A few observations further underline this claim.

Citation analysis is part of the academic science of bibliometrics, which is a set of methods used to study or measure texts and patterns of publication.<sup>15</sup>

In his 1955 paper Eugene Garfield, one of the founders of bibliometrics, actually used the already existent legal citation research tool, Shepard's Citations, to explain his then futuristic ideas of citation indexes for science.<sup>16</sup>

Today, those citation indexes have long become reality in many research areas and their use has been expanded to improving text retrieval systems in various areas. In the legal domain, however, the use of Shepard's citations as a mere reference collection has stayed the same, except for the

---

<sup>14</sup> P. ZHANG & L. KOPPAKA, "Semantics-based legal citation network", In *Proceedings of the 11th international conference on Artificial intelligence and law*, Stanford, California: ACM, 2007, pp. 123-130, at p. 123.

<sup>15</sup> . FEATHER & R.P. STURGES, *International encyclopedia of information and library science* (2. ed), at p. 38.

<sup>16</sup> E. GARFIELD, "Citation indexes for science; a new dimension in documentation through association of ideas", *Science*, 122(3159), 1955, pp. 108-111, at p. 108.

possibility to use Shepard's online. The use of Shepard's has therefore remained limited, while the tools that it inspired have been, among other areas, been used to improve the performance of text retrieval in their respective areas.

Thus, it seems strange that legal citations are not used for indexing. Every single citation that an author includes in their texts can also be seen as an act of indexing. When authors put references in their work, they include terminological interpretations in their texts.<sup>17</sup>

Also, returning to the comparison of modern Web search and legal text retrieval, I want to highlight one more aspect of legal citations. Google has shown us that link analysis in Web search has the potential to greatly improve search results.

As already shown, however, connections between documents are more central to the discipline of law than they are to any other field. Lawyers, legal scholars, and judges all pepper their writings with links to earlier sources, the only difference being that these links are called "citations" or "quotations."<sup>18</sup>

In fact, one might even argue that tightly linked court cases have to be even more closely related than equally linked Web pages: Citations within court decisions are nothing but arguments themselves. Citations have to persuade higher courts that the decision the judges made was correct. Therefore, judges have strong motivations to include citations thoughtfully.<sup>19</sup>

## **VI. CASE STUDY: AUSTRIAN SUPREME COURT DECISIONS**

In order to show that there is a direct correlation between the number of citations to legal documents and their legal impact, I have started to conduct a study with Austrian Supreme Court cases.

At [www.ris.bka.gv.at](http://www.ris.bka.gv.at), the Austrian Federal Chancellery operates the Legal Information System of the Republic of Austria ("Rechtsinformationssystem", abbreviated "RIS").

The objectives of RIS have been to provide up-to-date and exhaustive legal

---

<sup>17</sup> E. GARFIELD, "Citation indexes for science; at p. 110.

<sup>18</sup> F.R. SHAPIRO, *Collected papers on legal citation analysis*, Littleton Colo.: F.B. Rothman., 2001, at p. 161.

<sup>19</sup> T.A. SMITH, "The Web of Law", at p. 345.

information in an electronic format to both state organs and the general public.<sup>20</sup>

Another objective of providing "cost effective legal information"<sup>21</sup> has become obsolete because since 1997 the respective content of RIS has been accessible for everyone free of charge via the Internet.

The RIS application "Case Law" ("Judikatur", <http://www.ris2.bka.gv.at/Judikatur/>) contains - among other documents - the full texts of the Austrian Supreme Court decisions. The RIS system is, however, able to provide not only the full texts of the decisions, but also headnote documents created by the Publication Office of the Supreme Court. Each decision document is intellectually processed by a legal specialist at the court, and if a decision has introduced a new interpretation of Austrian legal statutes, special headnotes called "Rechtssatzdokumente" are created and cite to the respective court decisions.

Using a document collection that consists of more than 100,000 full-text decision and headnote documents, I have constructed a network of all Austrian Supreme Court cases since 1985.

Although various practical problems did arise, my methodology has been quite simple so far: The computer code I developed counts the number of citations from within headnote documents to Supreme Court decisions, and ranks the court decisions according to their citation totals. By doing that, I was already able to show - for the first time - that this network is a scale-free one, which means that a few court decisions have many headnotes attached to them, while most decisions have only a few headnotes, or none at all. This observation by itself already suggests further looking into the possibility of using Web search ranking algorithms in legal information retrieval systems, because the network structure of the World Wide Web is a scale-free one as well.

I am now turning to traditional indications of impact concerning Supreme Court cases, including the publication in an official legal reporter or high citation counts in annotated codes. By examining the cases returned by those means of traditional legal research with respect to their position in the "Web of Supreme Court Cases", I will be able to further explore the

---

<sup>20</sup> BUNDESKANZLERAMT, *Rechtsinformationssystem des Bundes: RIS ; eine kurze Einführung*, Wien: Bundeskanzleramt-Verfassungsdienst, 1994, at p. 1.

<sup>21</sup> BUNDESKANZLERAMT, *Rechtsinformationssystem des Bundes: RIS ; eine kurze Einführung*, at p. 1.

exact nature of the correlation between the number of headnote citations to Supreme Court decisions and their legal impact.

## VII. CONCLUSIONS

Court cases, statutes and other legal authorities are linked together by citations. This legal citation network is in fact not only extremely large, but also one of the best-documented existing human-created networks.<sup>22</sup>

Legal text retrieval systems have not made any major changes to their search technologies within decades, although the shortcomings of current legal text retrieval have been well-documented.

This paper has set out that possible improvements for legal text retrieval constitute a necessary area for research, and that legal citation analysis can serve as a means to improve current systems.

Using only freely available data from the Legal Information System of the Republic of Austria, I have been able to show that the network structure of Austrian Supreme Court decisions and their headnotes is similar to the one of the World Wide Web. This already suggests the general feasibility of using Web ranking algorithms in legal information retrieval systems. The next step will be the computation of a more sophisticated automated ranking of Austrian Supreme Court cases that is fully in line with methods of traditional legal research.

---

<sup>22</sup> T.A. SMITH, "The Web of Law", at pp. 310-311.

# TOOL-SUPPORTED LEGAL RISK MANAGEMENT: A ROADMAP

Tobias Mahler\*

## I. INTRODUCTION

In *The Future of Law*,<sup>1</sup> Richard Susskind predicts a paradigm shift in the approach to legal problems from *problem solving* to *problem prevention*:

“While legal problem solving will not be eliminated in tomorrow’s legal paradigm, it will nonetheless diminish markedly in significance. The emphasis will shift towards legal risk management supported by proactive facilities, which will be available in the form of legal information services and procedures. As citizens learn to seek legal guidance more regularly and far earlier than in the past, many potential legal difficulties will be dissolved before needing to be resolved. Where legal problems of today are often symptomatic of delayed legal input, earlier consultation should result in users understanding and identifying their risks and controlling them before any questions of escalation.”

This paper presents a roadmap towards a tool-supported legal risk management. Imagine a future in which some lawyers are also seen as *legal risk managers* by their clients or employers. Susskind considers the legal risk manager as one of the five main future roles for lawyers.<sup>2</sup> Such lawyers will specialize in the identification of legal risk and will be experts in the structured assessment and treatment of risk in the legal context. Those lawyers focusing on legal risk management will use specialized methods and software tools in their risk assessments. Again we can refer to Susskind:<sup>3</sup>

“This category of lawyer is sorely needed and is long overdue. Senior in-house lawyers around the world insist that they are in the business of legal risk management – clients prefer avoiding legal problems rather than resolving them. And yet [...] hardly a lawyer or law firm on the planet has chosen to develop methods, tools,

---

\* Norwegian Research Center for Computers and Law, University of Oslo, Norway. The work presented in this paper was kindly financed by the Norwegian Research Council under the ENFORCE project grant.

<sup>1</sup> R. SUSSKIND, *The Future of Law*, 1998, p. 290.

<sup>2</sup> See R. E. SUSSKIND, *The end of lawyers? Rethinking the nature of legal services*, 2008, p. 272.

<sup>3</sup> *Ibid.*, p. 272.

techniques or systems to help their clients review, identify, quantify and control the legal risks that they face. I expect this to change. [...] This could fundamentally change the way in which the law is practised and administered.”

The topic of the present paper is a set of potential future developments; however, I will seek to avoid making predictions. Of course, it is necessary to develop some assumptions about the future, but these are only extensions of current developments, without the addition of anything substantially new. Really new developments, particularly discoveries, are unforeseeable for epistemic reasons.<sup>4</sup> The present roadmap<sup>5</sup> for legal risk management is by no means a deterministic prediction, but should rather be read as a discussion of goals and ways to attain these goals. This roadmap should be seen as a contribution to a discussion about future *directions*, rather than as a literal map indicating the path itself. As Winston Churchill put it, plans are of little importance, but planning is essential. Planning views the future in a non-deterministic way, where we can influence central elements of future developments, despite the likely prospect that the plan itself may need to be adapted along the way.

## II. LEGAL RISK MANAGEMENT

This section introduces legal risk management as the proposed goal for this roadmap. Risk management is today used in many different disciplines as a structured approach for dealing with risk. Enterprise risk management focuses on risks to an enterprise, while financial risk management deals with risks, for example, in an investment portfolio. Engineers use risk analysis, such as to analyze the risk of technical failure of a system. The characteristic element in *legal risk management* is the focus on legal issues in the context of risk. This legal perspective on risk becomes visible in the management of *legal risk*<sup>6</sup>, a perspective which in itself is not new: practicing lawyers already deal with risks on a daily basis. The only proposed new elements are (1) the *conceptualization* of these activities as a type of risk management, (2) the search for more *structured methods* to carry out legal risk management tasks and (3) the possible development of *software-based tools* to support legal risk management.

The *conceptual question* is a contemporary rather than a future issue. As

---

<sup>4</sup> See N. N. TALEB, *The Black Swan: The Impact of the Highly Improbable*, 2008.

<sup>5</sup> See in general about technology roadmapping R. PHAAL, C. J. P. FARRUKH and D. R. PROBERT, ‘Technology roadmapping: A planning framework for evolution and revolution’, *Technological Forecasting & Social Change*, Vol 71, No 1-2, pp. 5-26.

<sup>6</sup> T. MAHLER, ‘Defining Legal Risk’, in: S. NYSTÉN-HAARALA ed, *Corporate Contracting Capabilities: Conference proceedings and other writings*, 2008, pp. 51-76.

Wahlgren<sup>7</sup> has indicated, some of the risk-related work tasks of practicing lawyers can be seen as a type of risk management. According to the ISO, the term “risk management” refers to “coordinated activities to direct and control an organization with regard to risk”.<sup>8</sup> By relating legal risk management to other risk management approaches, we may contribute to the development of a practical theory of proactive legal practice, which today is rather immature. There is an abundance of theory about how to interpret the law, once a problem arises. But legal theory has relatively little focus on how to avoid problems. Understanding and denoting some of lawyers’ tasks as risk management tasks provides us with a set of risk-related concepts and analyses, which may turn out to be helpful also for the analysis of legal risks.<sup>9</sup>

In my opinion, there are few alternatives to the conceptualization of lawyers’ risk-related tasks as legal risk management. When a lawyer analyzes potential risks (e.g., when drafting a contract) and how to avoid a negative outcome (e.g., when choosing the best wording for a contract), this may *also* be seen as *risk management*. However, the interesting question is not the conceptual or terminological issue of *whether* lawyers do risk management, but *how lawyers should manage risk*. The answer to this second question will be discussed in the remainder of this section. An analysis of legal risk management *methods* is a necessary basis for a discussion of possible legal risk management *tools*, which will follow in Section III.

#### 1. *Legal risk management methods*

Susskind’s future of law predicts that “legal risk management, supported by proactive facilities. . . will be available in the form of legal information services and procedures”. Could such *procedures* and *proactive facilities* for legal risk management be based on established risk management methods? There have been some suggestions in legal literature to use formalized risk management approaches in law<sup>10</sup>, but so far, legal risk management is, if

<sup>7</sup> P. WAHLGREN, *Juridisk riskanalys: mot en säkrare juridisk metod*, 2003.

<sup>8</sup> I.S.O., *Committee Draft 2 for Risk management - vocabulary*, Guide 73, 2008.

<sup>9</sup> See further T. MAHLER and J. BING, ‘Contractual Risk Management in an ICT Context – Searching for a Possible Interface between Legal Methods and Risk Analysis’, *Scandinavian Studies in Law*, Vol 49, pp. 339-358.

<sup>10</sup> See K. REID, *Risk-e-business: A framework for legal risk management developed through an analysis of selected legal risks in Internet Commerce*, University of New South Wales, 2000; WAHLGREN, *Juridisk riskanalys: mot en säkrare juridisk metod*, *supra* note 7; P. KESKITALO, *From assumptions to risk management: an analysis of risk management for changing circumstances in commercial contracts, especially in the Nordic countries: the theory of contractual risk management and the default norms of risk allocation*, 2000; P. KESKITALO, ‘Contracts + Risks + Management = Contractual Riskmanagement?’ *Nordic Journal of Commercial Law*, 2006, Vol 2 .

anything, still emerging as a methodological approach. The goal for legal risk management is to facilitate the management of legal risk. While risk management also may be carried out informally, there may be some situations and contexts in which a more formalized risk management process and established methods may be advisable. The term *method* is here used as a *codified set of recommended practices*. Interestingly, discussions of explicit practical proactive methods do not have a strong academic tradition in law. However, this does not necessarily indicate that a structured methodological approach is entirely irrelevant for, or inapplicable to, complex tasks typically carried out by lawyers. Rather, the lack of academic studies on practical methods seems to reflect the tradition of leaving the practical methods to the legal practitioners. However, given the increased complexity of legal practice in a diversified international context, it may nevertheless be useful to devote some research efforts to developing practical methods with clear interfaces to methods used in other disciplines.

a. Risk management

In general, risk management consists of one or more *risk assessments*. Typically, a risk assessment involves risk identification, risk estimation, risk evaluation and risk treatment. For example, a strongly simplified version of an engineering risk assessment may (1) identify the risk of a bridge collapse because it cannot withstand an earthquake (risk identification). Then, (2) the engineer would analyze the uncertainty and assess the likelihood and the consequences of a bridge collapse due to an earthquake (risk estimation). The next step (3) would be to assess whether this risk is acceptable (risk evaluation). Depending on the evaluation results, the engineer would then (4) proceed to discuss the effect and cost of possible technical or other measures to manage the risk (risk treatment). Could a similar approach be used to assess legal risk? This would require a risk assessment that not only focuses on factual events, but also on the application of legal norms to these facts. A legal risk assessment should assess how the application of legal norms may have an effect on the stakeholder.

I suggest as a starting point that a legal risk assessment should concentrate on the identification, estimation and treatment of legal risk. Thus, we need to clarify the meaning of the term “legal risk”.

b. Legal risk

There does not seem to be any agreement about the definition of legal risk

in literature and in practice.<sup>11</sup> In particular, it is not clear (1) whether legal risk implies that there must be uncertainty about the outcome and (2) whether this uncertainty must necessarily be legal uncertainty, or if uncertainty about facts is sufficient. For the purposes of this paper, I suggest the following working definition of legal risk: Legal risk refers to the risk related to a decision in a legal case.

Two observations should be made with respect to this working definition. First, this definition does not focus on how legal risk is caused, but rather on how legal risk materialises (in a legal case). Second, the definition depends on two other terms, namely “risk” and “legal case”, which both need to be clarified. There is no need to define risk differently than in other contexts, so I suggest we use the definition contained in the draft revision of the risk management vocabulary, issued by the International Organisation for Standardisation (ISO).<sup>12</sup> There, risk is defined as the “effect of uncertainty on objectives.” The use of this definition in the context of legal risk thus implies that also legal risk must be an effect of uncertainty. Uncertainty is defined by the ISO as the “state, even partial, of deficiency of information related to or understanding or knowledge of an event, its consequence or likelihood”. An *event* is, according to the ISO, the occurrence or change of a particular set of circumstances. Thus, in the context of legal risk, uncertainty could be the deficiency of information, understanding or knowledge of a legal decision, its consequences or likelihood. Now we need to introduce at least a preliminary definition of the term “legal decision”. For the purposes of this article, the term “legal case” refers to any type of decision about facts (circumstances), which is taken based on one or several legal norms.

The term “legal case”, as it is introduced here, is meant to include at least two types of rather distinct legal decisions. The *first* type of legal decision is the *legally binding decision* by an actor who holds a particular legal power. The ideal type of the binding legal decision is of course a judge’s judicial decision in a court case. However, other relevant decision makers could be authorities or even a third party, like a contract partner, who holds a particular legal power.

The second type of legal decision of relevance for legal risk is the decision which is taken by any actor *in light of the legal norms that apply to the decision*. This type of decision is much less formal and visible than the first type. The decision may not have to be conscious, and it may or may not even be

---

<sup>11</sup> MAHLER, *supra* note 6.

<sup>12</sup> I.S.O., *supra* note 8.

easily discernible in the actor's behaviour.<sup>13</sup> This type of decision is not characterized by its bindingness (even though it is possible that the decision has certain binding effects on others), but rather through the direct effect the decision has on the actor's behaviour. One example of this type of decision is a *compliance decision*.<sup>14</sup> The compliance decision is taken by the complying actor, based on the identified set of norms that apply to the decision. An example is my decision to pay a certain sum of money to someone else, *because* I am obligated to do so. Another example of this type of legal decision is the decision to *bear a negative outcome*, without making any legal claim (e.g. for compensation). In both examples, the actor acknowledges the binding force of the legal norms. For lack of a better name, such decisions will subsequently be referred to as an *actor's acceptance of consequences*.

We may ask why it is necessary to include this second type of legal decision when identifying legal risk. Isn't it sufficient to focus on the binding decisions of judges, authorities and others? Doesn't the bindingness of these decisions represent the core element of the law, as a set of binding rules? The answer is a rather simple combination of empirical facts and pragmatic judgment. *First*, very few legal problems are ever brought to court. In most cases we either comply immediately, or after some negotiations, or simply do not comply with the law at all. This needs to be taken into account when we identify how the law may have an effect on us in the future. *Second*, the actor's acceptance of consequences is included because its economic and other effects on the actor are to a certain degree comparable to binding legal decisions. From a practical perspective, I am affected both by a judicial decision which states that I have to pay a sum of money, and by my own decision to comply with my payment obligations. Of course, there are differences between the two types of decisions, and these should not be neglected. In particular, my own decision surely has an immediate effect on me, while a future judicial decision may be uncertain both in terms of whether I have to pay and how much I will have to pay. However, these differences do not justify omitting the second type of decision from the analysis of legal risk.

Instead, we should rather highlight how the two types of legal decisions

---

<sup>13</sup> The actor may (unconsciously) decide to do nothing. For example, an actor faced with an economic loss does not to make any claim, because no claim would have sufficient support in the law. It would be possible that the actor does not even think about the potential option of making a claim.

<sup>14</sup> A relevant question is how we should deal with non-compliance. Most likely, non-compliance has a different place in the context of legal risk. Non-compliance may be one of the causes of a legal risk, but not of the consequences. However, this aspect must be left open for the time being.

are connected. In the case of a binding decision, the actor is forced to consider the effects of that binding decision, particularly in light of a possible enforcement. If the binding decision does not directly initiate enforcement actions, then the actor is again faced with a decision about accepting the consequences of the decision. Thus, the actor's assessment of its options (including in particular to appeal, to do nothing, to await enforcement, or to comply) can again be characterized as the acceptance of consequences. The important point is that both types of decisions may have an effect on the actor's objectives. This potential future effect is the main reason why legal decisions are of key relevance to legal risk assessment.

c. Risk assessment method

One key difference between the example of engineering risk assessment and a lawyer's risk assessment is that lawyers typically do not follow a standardized method. However, the following *typical practice* may be discerned by comparing the above procedure to the steps that arguably will be followed by many lawyers when analyzing a future situation. Generally speaking, a lawyer might typically (1) identify risks, then (2) *analyse* how the relevant law (or contract) regulates the issue at stake (*hypothetical application of the law*), and then (3) evaluate whether the legal outcome serves the interests of the client, concluding by (4) proposing to *treat* the risk with adequate measures. These measures could then be implemented by the lawyer's client, based on an informal cost-benefit assessment, which also takes the legal validity of the measures into account. The key difference between the lawyer's assessment and the engineer's risk assessment lies in the fact that the lawyer typically does *not estimate the risk value*, that is, the likelihood and consequences of the risk. At most, the hypothetical application of the law will include an *estimation of a likely legal output*, which depends on legal uncertainty. However, this output is often not quantified in terms of consequences (e.g., financial) and a likelihood value.

Nevertheless, the above legal practice could be understood as a purely qualitative legal risk assessment method, which may be supported by some of the tools described in Section III. In addition, it might in some situations even be useful and cost efficient to go a step further and *estimate risk values*, as it is practised in other disciplines' risk management methods. In the following, I will exemplify how a full-scale semi-quantitative risk assessment method could be used to assess the clauses of a contract.<sup>15</sup>

---

<sup>15</sup> This section is based on T. MAHLER, 'How can we manage contractual risk?' *Contracting Excellence*, 2008, Vol 1, No 5, pp. 15-16.

## 2. *Example: contract risk assessment*

The method discussed below is based on an adaptation of existing international standards for risk management to the requirements of a contract analysis. The relevant standards include the Australian Standard AS 4360/2004 and the currently available draft version of the upcoming ISO standard 31000, "Risk management – Principles and guidelines on implementation". The process of risk management is a continuous one, which is carried out through *risk assessments*. If we want to examine a contract in a formalized risk assessment, then some of the steps specified in the above-mentioned standards need to be adapted. This article may be complemented with literature on the use of the Australian Standard, which explains the details of the general process that cannot be sufficiently covered here.<sup>16</sup>

A contractual risk assessment can consist of the following steps:

Specify the context, target and scope of the risk assessment. What exactly do you want to analyze?

Identify risk, that is, describe possible events and legal decisions (legal cases), based on the contract clauses as applied to the contractual relation. Based on the contract clauses and the business context, what legal decisions may have an effect on the stakeholder?

Estimate the likelihood and consequences (for example, monetary) of each identified risk. The estimation of likelihood should consider both the likelihood of facts and a relevant interpretation of the contract clauses.

Evaluate the risks, distinguishing between acceptable risks and those risks that should be considered for treatment. This evaluation should be based on both the risk values (that is, high or low risk) and a suitable set of decision criteria.

Consider how risks can be treated through practical measures or a suitable contract amendment.

The decision about treatment implementation depends on a cost-benefit analysis.

Consider the following scenario. The management at an automotive supplier requests that a lawyer assess the general purchasing terms and conditions of a car manufacturer. Let us assume that the supplier's management has had positive experiences with risk management in other

---

<sup>16</sup> STANDARDS AUSTRALIA and STANDARDS NEW ZEALAND, *Risk Management Guidelines Companion to Australian/New Zealand Standard AN/NZS 4360: 2004 (HB 436:2004)*, 2004. See also STANDARDS AUSTRALIA and STANDARDS NEW ZEALAND, *Legal risk management*, 2007.

contexts, and suggests that the lawyer use a standard risk management method. The overall objective is to negotiate a side letter, containing more beneficial terms and conditions regarding those contract clauses that imply too much risk. As a preliminary step in preparing and negotiating this side letter, the lawyer has to clarify *how risk management can be applied to contract drafting*.

The idea of relating contracting with risk management is in itself not new, but there is relatively little literature on how contractual risk management should be carried out in practice.<sup>17</sup> In the following, we will take a closer look at the steps introduced above as they relate to contractual risk assessments. The method has been applied in practical case studies, including the above-mentioned scenario, and is currently under evaluation.

a. Context, target and scope

Every risk assessment should start with specifying its exact scope and target, which in our context needs to be related to the rules in a contract. Depending on the time available and the importance of certain issues, the risk assessment could *target* either the whole contract or selected parts of it. Of course, if parts of the contract are excluded from the formal risk assessment, they should still be assessed less formally outside the risk assessment. The *scope* of the assessment depends on the client's requirements to cover, for example, certain types of risks or to analyze a particular set of documents. It may be necessary to spend some time on establishing the *context* and describing what the contract aims to regulate. Preferably, this background information should be well-documented and available for review during the remaining assessment steps.

The quality of the risk assessment results depends to a large extent on the available experience about, and knowledge of, the domain in question. Typically, few individuals have a comprehensive understanding of all relevant aspects of a complex business contract. A lawyer is competent to analyze the contract clauses, but often lacks detailed operational knowledge. Similarly, technical experts may lack detailed information about the financial and legal consequences of technical problems. For complex commercial contracts it may therefore be advisable to carry out a contractual risk assessment with a suitable *inter-disciplinary team of experts*, covering, for example, legal, financial, technical, market and other

---

<sup>17</sup> See in detail, T. MAHLER, 'The State of the Art of Contractual Risk Management Methodologies', in: H. HAAPIO (ed), *A Proactive Approach to Contracting and Law*, 2008, pp. 58-72.

perspectives.<sup>18</sup> A lawyer with experience in risk management could lead the assessment if the main focus is on legal aspects.

Every risk analysis focuses on identifying events (including legal decisions) that may impact the client's objectives or key assets. Therefore, the assessment should specify what the client wishes to protect, by listing relevant *objectives* (including the protection of its *assets*). It is also useful to initially set out how risk will be documented and measured (for example, quantitative or qualitative *risk values*) and what *criteria* for risk evaluation the client wishes to use. Guidance on the latter questions is available, for instance, in literature on the use of the Australian Standard for risk management.<sup>19</sup>

#### b. Risk identification

The second step consists of identifying the risks. In general, this involves identifying what, why, where, when and how *events* could impact the achievement of the organization's objectives or the value of its assets. In the context of a contract draft, we are particularly interested in legal decisions that are based on the contract text. Therefore, one possibility for risk identification is to analyze one clause at a time, seeking to find out *how each clause could lead to a legal decision that impacts the organization's objectives or assets*. In practice, this involves brainstorming about likely facts and subsequent decisions that could negatively impact the client's objectives. In this context, the risk identification also needs to consider the *interplay between different contract rules*, which may be relevant to a legal decision. For many decisions, several clauses need to be read in a suitable combination. For example, the contract may include a clause that obligates the supplier to pay consequential damages in case of delay. In order to assess the risk, the analysis of course also needs to assess what impact the applicable law and other relevant material may have on the rights and duties of the contract parties. The outcome of this step is a list and a description of possible future legal "cases", which should include a description of both the anticipated facts and the likely legal assessment thereof. Such "cases" may be either binding decisions by courts or other authorities, or the actor's acceptance of consequences, in recognition of the legal norms included in the contract or in the background law.

---

<sup>18</sup> However, the costs of such a comprehensive analysis will only be justified for exceptionally high-value or high-risk contracts.

<sup>19</sup> See e.g. STANDARDS AUSTRALIA and STANDARDS NEW ZEALAND, *Risk Management Guidelines Companion to Australian/New Zealand Standard AN/NZS 4360: 2004* (HB 436:2004) .

c. Risk estimation and evaluation

The analysis could subsequently make an effort to estimate the likelihood and consequence values for all identified legal decisions. The *consequence* value is an estimation, for example, of the monetary consequence of the legal decision. The *likelihood* value is an estimation of the frequency or probability of the decision. The likelihood of the decision may directly depend on the rules contained in the contract. Because the interpretation of the rules is not always certain, this uncertainty should be directly included in the analysis. The likelihood of the legal decision may thus depend on *likely facts* and a *likely interpretation of the contract*. For example, the analysis can combine the assessment of the *factual* likelihood of a delay with an estimation of the *legal* likelihood of a particular contract interpretation that implies a payment obligation in case of delay. For example, the legal likelihood may be that it is unlikely that the contract can be interpreted to the effect that the client has to pay damages for delay. Likelihood values can be combined based on the basic rules of probability, which can not be covered in any detail here.<sup>20</sup>

The combination of *likelihood* and *consequence* values renders the risk value, according to which the analyst can prioritize the risks. Subsequently, the team should *evaluate* which risks can be accepted, for example based on their low risk value, and which need be considered for treatment. This evaluation should be based on the client's risk appetite, the balance of risks and benefits in the contract and other criteria, for example, the degree of influence the client has on the manifestation of the event. However, great care has to be exercised with the use of risk values. If the empirical basis for the risk estimation is shaky, as will often be the case in the early phases of a contractual relation, then one should be even more cautious about understanding risk values as reliable and exact predictions of the future. Rather, the risk values should be used as one out of several relevant inputs in a discussion about adequate risk treatment measures.

d. Risk treatment and cost-benefit

The final phase focuses on how the identified risks can be treated. There are two key types of treatment of particular relevance to contracts. First, the risk may be treated by *practical measures* that ensure that a particular legal decision is less likely to happen, or will be less costly. Second, it may be possible to *amend certain contract clauses during contract negotiation*. For example, if the contract includes a clause about consequential damages in case of delay, and the risk analysis team considers that there is a risk that the supplier will have to pay a substantial sum in damages for delay, then

---

<sup>20</sup> For details see I. HACKING, *An introduction to probability and inductive logic*, 2001.

the treatment options include both contract amendment (e.g. liability limitation or liability exclusion, the details of which depend on the applicable law) and practical measures to reduce the likelihood of delays. The choice among the treatment options depends on a *cost-benefit analysis*. The benefit corresponds to the anticipated effect of the treatment on the risk level. This benefit needs to be related to the estimated cost of implementing the treatment. The cost-benefit analysis thus results in a recommendation of actions to manage the identified risks, which can be presented to the decision maker.

### 3. *A methodological supplement*

It is difficult to anticipate the potential role of the above introduced approach within the portfolio of proactive legal methods available to lawyers. Today, there is no standard way of analyzing risk in a legal context.<sup>21</sup> While engineers, IT security experts and enterprise risk managers are increasingly using standardized assessment methods, we lawyers seem to use experience-based heuristics to manage complexity and risk. This established approach has worked well in the past, and we should be very cautious about replacing it. In fact, given the immaturity of methods for legal risk management, it is so far an unrealistic alternative for the daily practice of most practising lawyers. Structured legal risk management should *not replace* existing legal methods, but it could support and accompany existing approaches as a supplementary method. The above described semi-quantitative method for contract risk assessment could be used in a situation where:

there is a need or desire to obtain a more comprehensive and detailed understanding of the risks inherent in a contract compared to a traditional non-formalized analysis;  
the contract text is stable during a sufficient time to carry out the analysis; and  
sufficient time is available for a detailed assessment — the necessary time depends on how selectively the assessment scope is chosen, but the required time for a detailed risk assessment could easily be several times the duration of a traditional contract analysis.

Legal risk management methods may be used for other purposes besides contract analysis. There are several incentives for adopting a structured approach to legal risk management. For example, in an enterprise risk management (ERM) assessment, the general counsel of a company may be asked to identify and estimate risks within his or her field of responsibility. In this case, the general counsel would need to follow the established

---

<sup>21</sup> MAHLER, *supra* note 17, pp. 58-72.

ERM method to identify and estimate risk. The need for sufficient overall risk management in a company may subsequently require the law department to identify and estimate risk in their daily practice in order to be able to report consistently. The dynamics of the largely soft-law based trend towards ERM and its implications for legal practice are difficult to anticipate. In some countries, including Germany, some companies are already required by law to have consistent ERM systems. Such requirements could be extended in the future.

Similarly, a systematic approach to risk management may be requested by customers of legal services. For example, the handbook for legal risk management, issued by Standards Australia and Standards New Zealand, encourages its readers to request that their legal advisors follow a systematic risk management approach.<sup>22</sup> However, a key problem with risk management is that it is rather time-consuming, costly and complex. Therefore, any success of the methodological approach may partly depend on adequate and efficient tools.

### III. TOOLS FOR LEGAL RISK MANAGEMENT

Risk management is cognitively challenging because the analyst and any other involved experts typically need to handle and take into account a rather complex set of statements about what may happen in the future, in addition to estimations of possibly dependent values of likelihood and consequences. Therefore, risk managers often use targeted software tools, which simplify risk identification, estimation, evaluation, treatment and, not least, communication. Of course, because enterprise risk management and financial risk management are carried out differently, they are supported by specialized tools — the same would have to be true for legal risk management.

How could the above introduced method for risk management be supported by tools? I will propose three complementary approaches, which could be implemented in combination or separately. The three approaches follow naturally from the risk management method. The keywords are (1) legal risk management *procedures and processes*, (2) support for the difficult tasks of risk identification and estimation, which may involve communication between lawyers and non-lawyers, and (3) the implementation within, or interoperability with, existing legal information systems. Moreover, all three types of tools or systems may cautiously introduce selected elements of automation.

---

<sup>22</sup> STANDARDS AUSTRALIA and STANDARDS NEW ZEALAND, *Legal risk management*.

1. *Legal risk management process and administration*

Tools that structure, simplify and facilitate a coherent analysis are often used to support risk management in other fields. Typically, risk managers need to capture and document the identified risks, their values and potential treatments. These administrative functions are already available in existing risk assessment tools. A good risk assessment tool assists the risk analyst in carrying out the relevant analysis steps in a suitable order, and helps to document all results in a consistent way, ideally in a reusable fashion. However, existing tools are insufficient in a legal context, because legal aspects are typically not adequately integrated into these analyses. Moreover, most risk assessment tools are discipline specific and focus on financial, technical or other issues. Nevertheless, tools from other disciplines, in particular enterprise risk management, might be adapted or extended to support legal risk assessments.

2. *Graphical tools to support risk identification and assessment*

The second type of tools is likely to be more challenging than the above process and administration tools. Risk analyses often involve brainstorming activities in interdisciplinary groups of experts. This part of risk analyses is often rather difficult, because it requires (1) discussions and agreement about what may happen in the future, (2) the intellectually challenging estimation of probabilities and (3) the estimation of financial or other consequences of events. Different experts will often have diverging views about all of these aspects. This is arguably even more difficult if the risk estimation is not limited to the likelihood of “facts” but also includes the likelihood of “legal outcomes”.

For example, imagine a company that wishes to assess the risk of a particular technical failure leading to liability according to the clauses of a major contract, in the context of the applicable background law. In this example, an engineer would be able to estimate the likelihood of the technical failure, and a lawyer may need to be consulted when the legal consequences are assessed. In the same example, the risk analysis might also need to assess the legal and contractual consequences of market changes, e.g. major raw material price increases. In this case, it would be useful to convene lawyers, engineers and managers together, in order to discuss and estimate the risk consistently. This clearly requires communication and mutual understanding of the others’ disciplinary perspectives. Of course, such communication already happens, and is often successful. However, sometimes such communication may be challenging due to the different methods and concepts used by the different disciplines. Just imagine a meeting where the lawyer brings the customer’s

general terms and conditions of purchase, under which the product will be supplied (45 pages), together with a book about the applicable law. The manager or the chief risk officer presents a set of spreadsheets that include financial information and risk estimates. The engineer contributes a set of technical drawings and the results of the engineering risk analysis (e.g. a failure modes and effects analysis, FMEA). Such an imaginary, but not unrealistic, meeting illustrates the clash of intellectual concepts behind the different disciplines which need to participate in the risk assessment.

My (unverified) impression from talking to managers and engineers in several companies is that *such meetings often do not happen* at all. Instead, the manager would at best send an e-mail to the lawyer, who then assesses the contract separately, with limited or no regard to the business and technical issues at stake.<sup>23</sup> At worst, the lawyer will not at all be consulted by the decision maker, perhaps to avoid a delay in the contracting process or in anticipation of an incomprehensible and lengthy legalese statement, which is not related to the technical and business issues at stake.

This *communications problem* may be amongst the *causes* for Susskind's observation<sup>24</sup> that "legal problems of today are often symptomatic of delayed legal input". Susskind assumes that "earlier consultation should result in users understanding and identifying their risk and controlling them before any question of escalation." However, if communications problems are amongst the causes for *delaying* legal input, then these communication problems may need to be addressed by lawyers and their customers or colleagues. The difficult communication regarding identified risks, their estimation and treatment needs to be supported by a number of complementary approaches, including education, improved internal culture in an enterprise and, possibly, IT tools.

*Tools for communication support* should of course be inspired by solutions that have proved successful in other disciplines. In computer science, graphical models are often used in systems design and analysis to illustrate the intended functions of the IT system. The Unified Modelling Language (UML) is a graphical language used for visualizing, specifying, constructing and documenting the artefacts of a software-intensive system. The UML offers a standard way to write a system's blueprints, including conceptual aspects such as business processes and system functions as well as concrete features such as programming language statements, database schemas and

---

<sup>23</sup> Such an assessment is likely to follow the traditional method as introduced above, in the introduction to section II.1. This may, of course, be sufficient for standard cases. However, if the issues are complicated and the law department or law firm has little experience with this type of business, more communication may be necessary.

<sup>24</sup> *Supra* note 1.

reusable software components.<sup>25</sup>

*Visualization* is an interesting approach in the legal context because some of the problems outlined above are not that different from the underlying analytical challenges of IT systems development, despite the obvious differences. IT systems development needs to deal with complex technical issues related to hardware and software, and the end product is essentially code, which may be unreadable by humans. This code has a mathematical and logical basis, but what counts is ultimately whether the IT system fulfils the users' requirements, i.e. whether the system works for and with human beings. The latter aspect is captured best in graphical models, which can be understood by non-experts who participate in the specification of the system requirements. Because the code may be illegible, one uses simple graphics to facilitate informed decision making during systems development.

*Code* is not an unknown concept for lawyers, as observed by Lawrence Lessig,<sup>26</sup> who refers to laws as "east coast code" and to technology as "west coast code". However, problems with the readability and understandability of code are treated rather differently in computer science and in law. This is obviously partly related to the fact that source code is not written in natural language and thus may be both *highly complex* and *very difficult to read*, while legal texts do use natural language. Legal texts may be *difficult* to understand for the inexperienced, but they should normally not be completely incomprehensible (even though there are sufficient examples of incomprehensible legalese nonsense).<sup>27</sup> Moreover, it cannot be neglected that understandability problems arise for completely different reasons. In most cases, "legalese" is used as a matter of tradition, and legal terms are used because of their specific legal meaning in the relevant legal community (as a *terminus technicus*). However, in some cases, the use of excessive legalese may even be employed as a strategy to inhibit the other party from understanding and appreciating its risks.<sup>28</sup> In any case, legal work also has to face the problem of code which is difficult to read,

---

<sup>25</sup> For an introduction to the UML, see [www.wikipedia.org](http://www.wikipedia.org). For more details, see M. FOWLER, *UML distilled: a brief guide to the standard object modeling language*, 3<sup>rd</sup> ed., 2004.. A comprehensive work is J. RUMBAUGH, G. BOOCH and I. JACOBSON, *The unified modeling language reference manual*, 2<sup>nd</sup> ed., 2004.

<sup>26</sup> L. LESSIG, *Code version 2.0*, 2006.

<sup>27</sup> An example can be found in C. KESSEL and V. PASSAUER, 'Einkaufsbedingungen in der Automobilindustrie' *Betriebsberater*, 1974, Heft 37.

<sup>28</sup> However, e.g. under German law, the issuer of general terms and conditions "bears the risk" of including an unclear clause, since the courts are reluctant to reduce such a clause to a valid and clearer one, see BGH ZIP 2007, p. 31 = *Betriebsberater* 2007, p. 177.

understand and evaluate from the perspective of risk. Nevertheless, lawyers have traditionally been reluctant to introduce (standardized) graphical models to understand, analyze and manage complex legal issues. There may be many reasons for this, not least the lack of availability of such graphical models. However, in addition there may be some underlying problems that could inhibit a modelling approach. Again, the *qualitative perspective* in legal reasoning may make it difficult to press law and justice into formalized and partly quantitative models. Even so, we cannot assess the potentials and limitations of graphical modelling for legal risk management before we have developed and tested such systems.

In risk management there is also an extensive use of graphical visualization methods to support risk assessments. For example, fault trees or Bayesian networks can be used to estimate the likelihood of a risk event. In the following I will sketch a possible approach for the visualization of legal risk. This is illustrated in Figure 1. The graphical models used here are based on the above introduced concepts of legal risk management, which are an extension of the ISO vocabulary for risk management.<sup>29</sup>

The lower part of the figure is essentially a simplification and adaptation of the CORAS language for security risk assessment, developed by computer scientists and inspired by the UML.<sup>30</sup> This part of the figure reads as follows. The event *e* (described in the leftmost vertex), which has the estimated likelihood *l*<sub>1</sub>, leads to the effect *f* on objective *o* (described in the rightmost vertex). This effect on the objective can be quantified by the estimated values for likelihood *l*<sub>3</sub>, consequence *c* and their combination, *v*.

The upper part of the figure illustrates how the effect is achieved *because* a legal norm *n* is applied to the circumstances of the case, i.e. the event.<sup>31</sup>

<sup>29</sup> This paper is based on draft risk management vocabulary, see I.S.O., *supra* note 8. The latter was chosen, rather than the currently valid version (ISO 2002), because it is likely that this draft will be adopted in the near future. Implicitly, I accept the risk that the ISO may deliberate differently.

<sup>30</sup> F. VRAALSEN, T. MAHLER et al, 'Assessing Enterprise Risk Level: The CORAS Approach', in: D. KHADRAOUI and F. HERMANN eds, *Advances in Enterprise Information Technology Security*, 2007.

<sup>31</sup> This part of the model is inspired by Toulmin's model of legal arguments, see S. E. TOULMIN, *The Uses of Argument*, 2003. For a critique of Toulmin's argument model, see J. B. FREEMAN, *Dialectics and the macrostructure of arguments a theory of argument structure*, 1991. The Toulmin scheme exists also in other variants, see G. KREUZBAUER, 'Visualisierung juristischer Argumentation', in: E. HILGENDORF ed, *Beiträge zur Rechtsvisualisierung*, 2005. The Toulmin approach has even been suggested as a basis for risk-based negotiation and decision support systems, see J. ZELENKOW, 'Risk, negotiation and argumentation—a decision support system based approach', *Law, Probability and Risk*, Vol 1, No 1, p. 37.

The legal norm is derived from a legal source *s*, which may be any source of law or a contract. If there is uncertainty about the norm, then this uncertainty may also be expressed by adding likelihood value to the norm. This likelihood is in Figure 1 referred to as likelihood  $l_2$ .

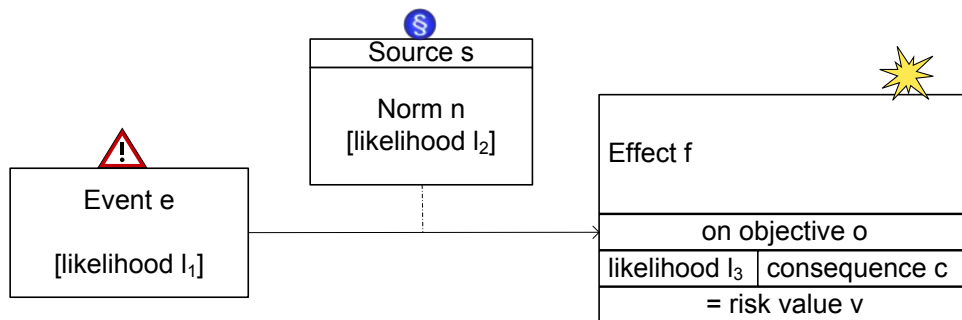


Figure 1 – Modelling legal risk

An example of a simplified legal risk diagram regarding a contractual obligation to pay consequential damages is provided in Figure 2 below. The diagram is meant to illustrate the following risk. In the unlikely event that a delivery is sufficiently delayed to result in loss of profit on the part of Buyer, Seller may decide to pay damages. The payment of damages is based on the contractual obligation to pay consequential damages, including loss of profit in cases of delay. The monetary consequences of the decision (a moderate consequence on the profits from this project) are a result of the identified factual event and the application of the legal norm to these facts. The likelihood of the decision depends on the likelihood of the initiating factual event, and the assessment of Seller's obligations in this event. The model in Figure 2 is simplified in order to illustrate the main features of the modelling approach. In particular, it would be possible to decompose the initiating event by adding further initiating events that contribute to the delay and to add further consequential events and decisions.

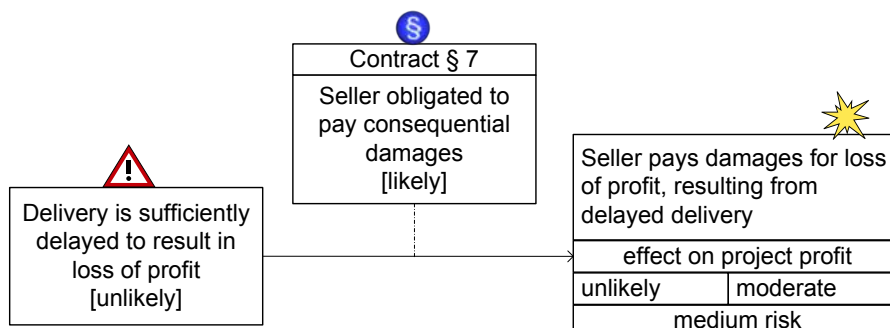


Figure 2 – The risk of obligation to pay damages for delayed delivery

The above examples are insufficient to conclude whether this preliminary graphical modelling language as such is useful. However, the diagrams are only included here as *examples* of graphical models that could support a legal risk assessment. This is a tentative suggestion rather than a comprehensive solution to our problem.

This modelling approach is intended for the type of interdisciplinary legal risk assessment meeting described above. A previous (and more complex) version of the graphical language was tested in a full-scale industrial case study. Of course, the models imply a significant need for simplification, and the risk of over-simplification. However, this is a necessary consequence of introducing a model. If our limited brain resources could deal with all aspects of a complex reality, both today and in the future, then there would be no need for modelling. However, because we have to take bounded rationality<sup>32</sup> into account, some degree of selective simplification may in some situations be better communication rather than the full complexity of lengthy legalese documents. In any case, graphical models are not necessarily intended to be used instead of detailed legal analyses, but rather as an additional instrument to communicate a summarized result. If the output of a legal analysis is summarized in a concrete statement about risk and available options to manage such risk, then this output may be better understood and more easily used and implemented by non-lawyers. A suitable graphical legal risk management tool could therefore provide a simpler interface between the legal analyses and the risk analyses carried elsewhere in the organization. Graphical models alone will not solve the problem of delayed legal input, but if successful they may be amongst the measures that can partly solve some of the communication difficulties during legal risk identification and assessment. This again might contribute to an increased and earlier consultation of lawyers, as intended by Susskind.

### 3. *Risk management and legal information systems*

---

<sup>32</sup> The concept of bounded rationality is used to question the assumption, made in traditional economics and other sciences, that humans can be reasonably described as 'rational' entities (for example in rational choice theory). Instead, bounded rationality theory seeks to account for the fact that perfectly rational decisions are often not feasible in practice due to the finite computational resources available for making them. This has also consequences for the way risks can be analyzed and described. For example, a recent article describes the communications problems when discussing medical risk assessments, and discusses ways for simplified and still correct presentation of a medical doctor's risk estimates, see G. GIGERENZER and A. EDWARDS, 'Simple tools for understanding risks: from innumeracy to insight', *BMJ*, 2003; 327:741-744, doi: 10.1136/bmj.327.7417.741.

Ideally, any support tool for legal risk management should be integrated or interoperable with a law department's information systems. Today, these include at least (1) legal information systems and (2) contract management systems.

First, law firms and law departments use a variety of legal information systems to retrieve legal information like statutory or case law, soft law (codes of conduct), contract templates and legal literature. Some systems already include a limited functionality for contract drafting, based on contract templates. Moreover, some of these systems already include modules which bare the title "legal risk management". The latter typically includes checklists or similar tools to support day-to-day legal work. One example of a risk assessment tool is a German tool on a set of CDs entitled "tool-box of international trade law", where the user of the "risk analysis tool" can retrieve information about particular legal questions relevant to international trade law, with respect to a number of jurisdictions.<sup>33</sup> This type of tool may thus be used to estimate the legal outcome of a standardized set of facts, which are relevant to international trade. However, the tool only focuses on providing rather limited information and thus only covers a minor part of the overall risk management process, and does not offer any support for risk estimation and evaluation in general. Nevertheless, legal risk management tools could in the future be integrated or made interoperable with relevant legal information systems.

The second type of system, which could be a candidate environment for legal risk management tools, could be contract management systems. In general, contract management is the administration of an organisation's contracts. Contract management includes negotiating the terms and conditions in contracts and ensuring compliance with these, as well as documenting and agreeing to any changes that may arise during its implementation or execution. Today, contract management is in many organisations still carried out in manual processes without dedicated systems. However, e-mail negotiations and paper archiving routines often lead to poor availability of contracts in an organisation. Contract management software promises to solve this problem. Contract management software is intended to support contract creation, to ensure the availability of contracts and to support contract analysis. There are different approaches to contract management, but most contract management systems today allow a selected number of users to upload and change contracts, which then are made available for other users in the

---

<sup>33</sup> VERWEYEN, FOERSTER and TOUFAR, *Tool-Box des Internationalen Warenkaufs UN-Kaufrecht (CISG)*, 2008.

company.<sup>34</sup> Currently, contract management systems seem to provide limited support for risk assessment. However, in the future, such functionality could and should be added to contract management systems. The contract management system could, for example, assist in assessing the risk in a particular contract text that was uploaded into the database. Moreover, once the risk is identified and assessed, the results of the risk assessment could be used as meta information about the contract, which is documented and available for future reporting and other uses. The identified risks may thus be monitored adequately. The identified risk may also be relevant for the analysis of other comparable contracts, where similar risks could be identified. Thus, it could become possible to consistently manage the risk present in a portfolio of contracts.

#### 4. *A cautious approach towards automation*

Lastly, it may be possible to cautiously introduce selected elements of automation into legal risk management systems. The need for caution is based on the fact that risk management, at least in the legal domain, needs to involve a considerable amount of human judgement, which is difficult to automate. Nevertheless, it might be possible to use automated systems to support human judgement and analysis. A cautious approach to automation could imply the use of text parsers, that is software for syntactic text analysis, e.g. to select rules that may be a source of legal risk. One option for automation could thus be that a tool extracts some of the conceptual notions<sup>35</sup> in legal texts, and makes the results available as a text paste option in a tool based on the above outlined graphical approach. Thus, the text “Seller obligated to pay consequential damages, including loss of profit” in Figure 2 could be extracted from the contract document, identified as an obligation and suggested as a text paste option in the diagram. This could save some time and improve consistency. Moreover, the transparency could be improved if the legal source quoted in the diagram could be made directly available as a link to the full-text version of the legal document.

## IV. OUTLOOK

Although there are a number of potential benefits to be obtained through the introduction and use of methods and tools for legal risk management,

---

<sup>34</sup> A list of contract management software providers is available at the website of the International Association for Contract and Commercial Management, [www.iaccm.org](http://www.iaccm.org).

<sup>35</sup> C. BIAGIOLI, E. FRANCESCONI, A. PASSERINI, S. MONTEMAGNI, C. SORIA, ‘Automatic semantics extraction in law documents’, *Proceedings of the 10th international conference on Artificial intelligence and law*, June 06-11, 2005, Bologna, Italy.

we need to acknowledge the significant difficulties and obstacles.<sup>36</sup> For one, lawyers are not trained in risk management methods, and are used to a substantial methodological freedom for all tasks outside the interpretation of the law. Moreover, law is often open to interpretation and legal decisions are not always predictable from the outset, so most legal risk assessments need to deal with rather uncertain assessments. Legal risk assessments may, in addition, be rather time consuming and costly. Consider, for example, the possibilities of failure in a major commercial contract. The consistent analysis of all risks may be more costly than the potential improvement of the contract. Therefore, it may only be cost efficient to carry out a full-scale risk assessment for contracts that either have an exceptional value or that are sufficiently representative of other, similar contracts, so that the risk analysis results also are useful for those contracts that are not analyzed in detail. Last, but not least, clients may be less interested in paying expensive lawyers for a proactive legal risk assessment, compared to a situation in which a risk has already materialized and they necessarily have to face a major and costly legal problem. As a business model, legal risk assessment may therefore have some limitations for law firms.

These obstacles and limitations need to be taken into account in any development of legal risk management methods and tools. Nevertheless, there is sufficient potential in legal risk management to justify further research. The real benefit of new methods and tools for legal risk management can only be verified by defining a method for legal risk assessment, together with initial tool support, and testing these in a suitable case study.

---

<sup>36</sup> See also WAHLGREN, *supra* note 7, pp. 133-145.

# PEEPING HALS: MAKING SENSE OF ARTIFICIAL INTELLIGENCE AND PRIVACY

Ryan Calo

## I. INTRODUCTION

The field of artificial intelligence, broadly defined as the study and practice of designing intelligent agents,<sup>1</sup> is at least six decades into its existence as a formal discipline.<sup>2</sup> Sometimes called “computational” or “synthetic” intelligence, AI borrows from and informs a wide variety of subjects, including philosophy, psychology, linguistics, neuroscience, statistics, economics, and law.<sup>3</sup> Techniques of AI underpin all manner of industrial and consumer applications—from the complex neural nets used in data mining, down to the ‘fuzzy logic’ used by commercial washers and driers.

Insofar as “the issues of AI are directly related to [the] self-image of human beings”,<sup>4</sup> and because the central projects and techniques of AI can often be articulated in lay language, few shy away from offering their insights and critiques.<sup>5</sup> This essay explores and updates a particular criticism—the long-standing claim that certain techniques and applications of AI violate human privacy—and discusses whether (U.S.) privacy law is adequately positioned to respond.

Historically, AI can be said to threaten privacy according to a specific pattern: AI substitutes for humans at various stages of observation or surveillance, allowing such activity to reach a previously impracticable scale. Whereas once telephonic surveillance required one listener per phone call, the development of voice recognition technology permits the substitution of a computer capable of monitoring thousands of calls

---

<sup>1</sup> S. RUSSELL and P. NOVIG, *Artificial Intelligence: A Modern Approach*, Saddle River, Pearson Education, Inc., 2003, pp. 1-2.

<sup>2</sup> The term “artificial intelligence” was coined by John McCarthy at the Dartmouth Conference in 1956. P. MCCURDOCK, *Machines Who Think*, Natick, AK Peters, Ltd., 2004, p. 529.

<sup>3</sup> *Id.*, pp. 5-16.

<sup>4</sup> H.R. EKBIA, *Artificial Dreams: The Quest for Non-Biological Intelligence*, New York, Cambridge University Press, New York, 2008, pp. 30-31. The author of this essay is no exception.

<sup>5</sup> See, e.g., MCCURDOCK, *Machines Who Think*, p. 406 (discussing Edward Fredkin’s concern that AI will hyper-concentrate power in the hands of one country or institution); B. JOY, “Why the Future Doesn’t Need Us,” *Wired Magazine*, Apr. 2000 (worrying aloud that AI will turn hostile toward humanity).

simultaneously.<sup>6</sup> Whereas once hundreds of intelligence analysts might be required to pour over field records in search of connections, AI knowledge management techniques automatically spot patterns and call them to the attention of agents.<sup>7</sup> These developments vastly amplifying the potential for data gathering and analysis, and hence underpin ubiquitous surveillance.<sup>8</sup>

Such advances in technology have played a key role in driving privacy law. The seminal 1890 article by Samuel Warren and Louis Brandeis, wherein the authors in many ways introduced a right to privacy protected by four causes of action, begins with a concern over “[r]ecent inventions and business methods” such as “instantaneous photography” that make possible previously unheard of behavior.<sup>9</sup> In the Fourth Amendment context, U.S. courts grapple with whether a given new technology permits humans to witness behavior in which, or occurring where, the individual has a reasonable expectation of privacy.<sup>10</sup> A state or federal regulator identify new information gathering practices—for instance, tracking online behavior for ad targeting—and hold it up against established fair information practice principles such as notice and control.<sup>11</sup>

A recent trend in AI complicates this dynamic. Increasingly, practitioners of AI and its subfield of robotics and human computer interaction are imbuing machines with ‘social’ characteristics.<sup>12</sup> These robots and computer interfaces contain key anthropomorphic signifiers such as eyes, expressive faces and gestures, and natural language capabilities designed to improve machine-human interaction. This set of techniques builds on extensive research suggesting that humans are exquisitely attuned to their own species, and that we react to computers, robots, and other social

---

<sup>6</sup> J. WEIZENBAUM, *Computer Power and Human Reason: From Calculation to Judgment*, San Francisco, W.H. Freeman and Company, 1976, p. 272.

<sup>7</sup> T. ZARSKY, “Mine your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in The Forum of Public Opinion,” 5 Yale J. of L. & Tech. 4 (2004), p. 4.

<sup>8</sup> *Id.*

<sup>9</sup> S. WARREN AND L. BRANDEIS, “The Right to Privacy,” 4 Harv. L. Rev. 193 (1890).

<sup>10</sup> See, e.g., *Kyllo v. United States*, 533 U.S. 27, 29 (2001) (discussing thermo-imaging devices).

<sup>11</sup> FTC Press Release, “FTC Staff Proposes Online Behavioral Advertising Privacy Principles,” Dec. 20, 2007, available online at <http://www.ftc.gov/opa/2007/12/principles.shtm>.

<sup>12</sup> T.M. HOLGRAVES ET AL, *Perceiving artificial social agents*, Computer in Human Behavior 23 (2007) 2163 (“One of the major trends in human-computer interaction has been the development of more natural human-computer interfaces”); *id.* at 2171 (“There is no doubt that this trend will continue to increase.”).

media as though it were actually human—including through the subconscious alteration of our attitudes and behavior. Its effect is to introduce apparent agents into a variety of new contexts.<sup>13</sup>

Some applications of social AI follow the original pattern of amplifying human capacities. For instance, commercial and governmental entities have begun to leverage social machines and software to stand in for marketers, recruiters, and other organization representatives in gathering information and influencing consumers and citizens. Just a single AI program—for instance, the U.S. Army's virtual recruiter "SGT Star"—can engage with thousands of individuals simultaneously and record every interaction. Thus, social machines can stand in for a human as interviewer or interrogator, preserving the persuasive skills of humans but adding additional advantages such as massive scale, tirelessness, and an essentially limitless memory.<sup>14</sup>

Other consequences of social AI, however, fall outside the prevailing pattern. Rather than standing in for some specific human task such as listening, pattern-spotting, or questioning, a machine that presents as an independent agent can stand in for a human *as subject*. That is, a humanoid robot's mere presence will signal to individuals that they are not alone, even if the robot is neither collecting nor evaluating information on behalf of a human, which in turn can sharply alter attitudes and behavior. Relatedly, where a computer interface engages with a user socially—a direction the global leader in Internet search expressly contemplates within the next few years<sup>15</sup>—extensive social science research shows that the individual will feel and react as though she is engaging with an actual person.

Although this set of applications does not augment the human capacity to observe in the tradition sense, it nevertheless threatens core privacy values.

---

<sup>13</sup> P.J. FOGG, *Persuasive Technologies: Using Computers to Change What We Think and Do*, San Francisco, Morgan Kaufmann Publishers, 2003, p. 10 ("With the growth of embedded computers, computing applications are becoming commonplace in locations where human persuaders would not be welcome, such as bathrooms and bedrooms, or where humans cannot go (inside clothing, embedded in automotive systems, or implanted in a toothbrush)."). See also H.R. EKBIA, *Artificial Dreams*, p. 8 (discussing fact that "[c]omputers are everywhere."); J. KANG and D. CUFF, "Pervasive Computing: Embedding the Public Sphere," 62 Wash. & Lee L. Rev. 93 (2005), p. 94 ("[T]he Internet will soon invade real space as networked computing elements become embedded into physical objects and environments.").

<sup>14</sup> P.J. FOGG, *Persuasive Technologies*, o.c.

<sup>15</sup> See <http://www.techcrunch.com/2008/12/10/marissa-mayer-at-le-web-the-almost-complete-interview/> (interview with Marissa Mayer).

As detailed below, a key role of privacy is to preserve solitude, in the sense of a temporary respite from interference with respect to curiosity, development, and thought.<sup>16</sup> Yet it is clear that people react to social machines as though they were human beings, including with respect to the sense of being observed. If, as many predict, social machines become ubiquitous—turning up in cars, bedrooms, bathrooms,<sup>17</sup> even within cell phones and mirrors<sup>18</sup>—possibilities for solitude may shrink intolerably. We may even witness a sea change of attitudes away from the prevailing view of computers as passive data conduits, in turn chilling curiosity at the borderline and creating discomfort around widespread machine custodianship of personal information.

It is exactly here, where AI begins to substitute for the human not as a gatherer or organizer of information but directly as subject, that privacy protections begin to break down. This is partly because American privacy law and theory focuses on the flow of information, on quantifiable harms, and on the level of notice and consent. It is also a function of limited imagination around the role of objects in our social lives. This essay concludes with thoughts on where to look in American law for legal analogues to vindicate the core privacy values threatened by social AI.

## II. TRADITIONAL INTERSECTION OF AI AND PRIVACY

On the traditional view, technology threatens privacy by increasing the power or reach of human observation. As prominent American privacy scholar Michael Froomkin sums up the space: “Privacy-destroying technologies can be divided into two categories: those that facilitate the acquisition of raw data and those that allow one to process and collate that data in interesting ways”.<sup>19</sup> Speaking on the subject of privacy invasive technologies, Harvard Law School’s Jonathan Zittrain identifies “three successive shifts in technology from the early 1970s: cheap processors, cheap networks, and cheap sensors”.<sup>20</sup> He continues that “[t]he third shift has, with the help of the first two, opened the doors to new and

---

<sup>16</sup> A. WESTIN, *Privacy and Freedom*, New York, Antheneum 1970, p. 35.

<sup>17</sup> P.J. FOGG, *Persuasive Technologies*, p. 10.

<sup>18</sup> P.J. O’RORKE, “Future Shlock,” *The Atlantic*, Dec. 2008 (“Various passages had caught my attention when I’d read it, and raised my blood pressure: ‘Closets will help pick out the right dress for a party.’ Imagine that: a talking mirror telling you, ‘That makes your butt look big.’”).

<sup>19</sup> M. FROOMKIN, “The Death of Privacy?,” 52 *Stan. L. Rev.* 1461, 1468 (2000). *But see id.*, pp. 1469-70 (acknowledging that “[f]or some, just knowing that their activities are being recorded may have a chilling effect on conduct, speech, and reading”).

<sup>20</sup> J. ZITTRAIN, *The Future of the Internet: And How to Stop It*, New Haven, Yale University Press, 2008, 205.

formidable privacy invasions”.<sup>21</sup> The thought is that humans will use cheaper and better technology to collect and organise information to greater effect, sometimes necessitating additional protections.

An early example of this analysis in the context of AI is synthetic intelligence pioneer Joseph Weizenbaum’s concern over the use of AI in data mining.<sup>22</sup> In 1976, Weizenbaum wrote a scathing critique of artificial intelligence along multiple lines. Weizenbaum had developed a program called ELIZA that was designed to mimic psychoanalysis by engaging in a credible dialogue with a human operator, in keeping with the “Rogerian technique of encouraging a patient to keep talking”.<sup>23</sup> ELIZA asked its users questions based on their previous answer and, where it did not have a response, merely supplied filler such as “I see” or “interesting”. Weizenbaum claimed that he was profoundly disturbed by the tendency of humans to react ELIZA as though it were a person, which prompted him to write a book about what computers should never be pressed to do.

In one powerful passage, Weizenbaum argues that the most obvious application of some artificial intelligence techniques is massive surveillance. Weizenbaum observes that, as of 1976, there were “three or four major projects in the United States devoted to enabling computers to understand human speech”.<sup>24</sup> According to the “principle sponsor of this work, the Advanced Research Projects Agency ... of the United States Department of Defense”, (now “DARPA”) potential applications were uncontroversial and benign. For instance, the Navy wanted voice recognition technology in order to “control its ships, and the other services their weapons, by voice commands”.<sup>25</sup> Weizenbaum rejects this explanation:

Granted that a speech-recognition machine is bound to be enormously expensive, and that only government and possibly a few very large corporations will therefore be able to afford it, what will they be used for? ... There is no question in my mind that there is no pressing human problem that will more easily be solved because such machines exist. But

---

<sup>21</sup> *Id.*

<sup>22</sup> “Data mining is correctly defined as the ‘nontrivial process of identifying valid, novel, potentially useful and ultimately understandable patterns in data.’ T. ZARSKY, “Mine your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in The Forum of Public Opinion,” 5 Yale J. of L. & Tech. 4 (2004), p. 6.

<sup>23</sup> J. WEIZENBAUM, *Computer Power and Human Reason: From Calculation to Judgment*, San Francisco, W.H. Freeman and Company, 1976, p. 3.

<sup>24</sup> *Id.*, p. 270.

<sup>25</sup> *Id.*, p. 271.

such listening machines, could they be made, will make monitoring of voice communications very much easier than it is now.<sup>26</sup>

Today, many varieties of sophisticated voice recognition technology exist.<sup>27</sup> Weizenbaum was wrong about the range of applications to which voice recognition would eventually be put—such technology has been used in everything from computers for the blind, to voice dialing, to hands-free wheelchairs. He was correct, however, that voice recognition would make massive government surveillance practicable.

Another concern closely related to Weizenbaum's insight that computers endowed with AI can stand in for human surveillants is the notion that AI can bring certain patterns of activity to the attention of humans. Thus, techniques of artificial intelligence have been used to decide where to point cameras or to 'flag' events such as the same face appearing in multiple transit stations. Weizenbaum hints in 1976 at this functionality as well:

Perhaps the only reason that there is very little government surveillance in many countries of the world is that such surveillance takes so much manpower. Each conversation on a tapped phone must eventually be listened to by a human agent. But speech-recognizing machines could [recognise and] delete all "uninteresting" conversations and present transcriptions of only the remaining ones...<sup>28</sup>

More recently, Israeli legal scholar Tal Zarsky discusses the power of AI to sift through and organise data in seconds that would take a human an eternity. Zarsky argues that "[m]ere surveillance ... is not grounds for concern, at least not on its own. The fact that there are an eye watching and an ear listening is meaningless unless the collected information is *recorded and emphasised*".<sup>29</sup> Zarsky goes on to provide a detailed description of "knowledge discovery in databases" (or "KDD"), in which "complex algorithms, artificial intelligence, neural networks and even genetic-based modeling ... can discover previously unknown facts and phenomenon about

---

<sup>26</sup> *Id.*, p. 272.

<sup>27</sup> See, e.g., Mass High Tech, "MIT adds robotics, voice control to wheelchair," Sept. 19, 2008, available online at <http://www.masshightech.com/stories/2008/09/15/daily64-MIT-adds-robotics-voice-control-to-wheelchair.html> (describing a voice-controlled wheelchair).

<sup>28</sup> J. WEIZENBAUM, *Computer Power and Human Reason*, p. 272.

<sup>29</sup> T. ZARSKY, "Mine your Own Business!," p. 4 (emphasis in original).

a database”.<sup>30</sup> These techniques are indeed central to AI applications, in which the ability to search for the right answer—particularly in a complex and even dynamic environment—is the key to performance.<sup>31</sup> After exploring the dangers of consumer and citizen data profiling, Zarsky concludes that greater public awareness of the AI techniques involved in data mining—well understood within, but not beyond, the field of computing—will lead to more ethical deployment of KDD.

Thus, according to Weizenbaum, Zarsky, and others, AI plays a role in supporting human surveillance that might otherwise prove impossible. The issue is considered serious enough that a popular AI textbook has cited the potential to invade privacy as one of six principle ethical questions around AI.<sup>32</sup>

### III. THE ROLE OF SOCIAL MACHINES

#### 1. *Robotics and computer interfaces*

A long-standing and accelerating goal of AI, especially within the subfields of robotics and human-computer interaction (“HCI”), has been to develop machines and programs that interact more naturally with humans. Due in part to increased worldwide demand for personal robotics (one research agency predicts that personal robotics will be a \$15 billion dollar industry by 2015),<sup>33</sup> roboticists have made close study of the human reaction to robots in the field. Some have reached the conclusion that humans are less likely to accept robots in certain capacities absent sufficient resemblance to humans and/or social complexity.<sup>34</sup> Thus, for instance, in developing the “Nursebot” Pearl for use in hospitals or elderly care facilities, researches at Carnegie Melon found that “if the Nursebot is too machine-

---

<sup>30</sup> Zarsky further observes that KDD can make predictions about the future. *Id.*, p. 8 (“After establishing the ‘clustering,’ both *descriptive* and *predictive* inquiries are possible.”) (emphasis in original). Beyond the scope of this essay is whether these techniques create new categories of relevant, invasive personal information that was never disclosed (or perhaps known) to the data subject.

<sup>31</sup> H.R. EKBIA, *Artificial Dreams*, p. 44.

<sup>32</sup> S. RUSSELL and P. NOVIG, *Artificial Intelligence*, p. 960.

<sup>33</sup> ABA Research, “Personal Robots Are Here,” New York, Dec. 28, 2007.

<sup>34</sup> See <http://robotic.media.mit.edu/projects/robots/mds/social/social.html> (“Given the richness and complexity of human life, it is widely recognized that personal robots must be able to adapt to and learn within the human environment from ordinary citizens over the long term.”); see also <http://robotic.media.mit.edu/projects/robots/leonardo/socialcog/socialcog.html> (“One way robots might develop socially adept responses that seem to reflect beliefs about the internal states of others is by attempting to simulate—in its own cognitive system—the behaviors of others.”).

like, her human clients ignore her, and won't exercise or take pills."<sup>35</sup> It was therefore necessary to make Nursebot appear more human and interact more naturally for it to be an effective tool in elderly care.

Other drivers behind socializing robots are the view that "to build systems that have human-level intelligence", it is necessary to "build robots that have not merely a physical body but in fact a humanoid form",<sup>36</sup> and the related hope that very complex behaviors can 'develop' over time through social interaction. Cynthia Breazeal, a pioneer in the emerging field of "social robotics" and the head of the influential MIT Media lab, has helped create a class of "Mobile/Dexterous/Social" robots capable of mimicking emotion and responding to social cues. In describing Kismet, among her first efforts in social robotics, Breazeal told the New York Times: "I hoped that if I built an expressive robot that responded to people, they might treat it in similar way to babies, and the robot would learn from that".<sup>37</sup> Her impressive work continues to advance in this direction.<sup>38</sup>

Software developers and computer engineers have similarly turned to more social interfaces. According to psychological science professor T.M. Holtgraves and colleagues, "[o]ne of the major trends in human-computer interaction ... has been the development of more natural human-computer interfaces".<sup>39</sup> Moreover, "[w]ith the advent of the Internet, the appeal of even more natural, human-like interfaces has increased dramatically".<sup>40</sup>

As a consequence of such research, the number of applications that leverage social dimensions is growing. Companies and other institutions make use of virtual representatives, discussed in greater detail below, in order to handle customer service calls and even sales and recruitment.<sup>41</sup> We are also seeing the deployment of human-like robots into a variety of spaces, including the home for entertainment and service.<sup>42</sup> Many

---

<sup>35</sup> P. MCCURDUCK, *Machines that Think*, p. 467. Conversely, the researchers worried that were Nursebot Pearl *too* humanlike, clients might form unnatural attachments to her. *Id.*

<sup>36</sup> H.R. EKBIA, *Artificial Dreams*, p. 259 (citing others).

<sup>37</sup> P. MCCURDUCK, *Machines that Think*, p. 454 (citing the New York Times).

<sup>38</sup> See, e.g., C. BREAZEAL, J. GRAY and M. BERLIN, "An embodied cognition approach to mindreading skills for socially intelligent robots," *International Journal of Robotics Research*, 2008 (to appear); A.L. THOMAZ and C. BREAZEAL, "Teachable robots: Understanding human teaching behavior to build more effective robot learners," *Artificial Intelligence*, vol. 172(6-7), 2008, p. 716-37.

<sup>39</sup> T.M. HOLTGRAVES et al., "Perceiving artificial social agents," *Computers in Human Behavior*, 2007, No 23, pp. 2163-2174, at p. 2163.

<sup>40</sup> *Id.*

<sup>41</sup> I. KERR, "Bots, Babes," *o.c.*

<sup>42</sup> P. MCCURDUCK, *Machines that Think*, p. 467.

computer systems, particularly those running on cell phones or in an environment that requires a ‘hands free’ user experience, have moved toward spoken language and other, more natural interfaces.<sup>43</sup> After some initial setbacks,<sup>44</sup> websites are becoming more interactive and personalised.

## 2. *Effects of social machines on humans*

It turns out that making robots and computers more social yields a profound effect on humans. Consider social scientist Sherry Turkle’s report after her encounter with the social robot Cog in the MIT Media Lab1990s:

Trained to track the largest moving object in its field (because that will usually be a human being) Cog “noticed” me soon after I entered its room. Its head turned to follow me and I was embarrassed to note that this made me happy. I found myself competing with another visitor for its attention. At one point, I felt sure that Cog’s eyes had “caught my own.”<sup>45</sup>

Studies across multiple disciplines have confirmed this human tendency to treat social objects as social, sometimes called the “ELIZA effect” in AI literature after Weizenbaum’s program.<sup>46</sup> In their influential book *The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places*, Byron Reeves and Clifford Nass detail their findings that humans treat computers as social actors.<sup>47</sup> Their method consists largely of reproducing experiments around known human behaviors toward other humans and substituting social computer for one set of people.<sup>48</sup> In this way, Reeves and Nass show that computers that evidence social characteristics have a similar, or, in some case, the exact same, effect on humans. Computers programmed to be polite, or to evidence certain personalities, have profound effects on test subjects.<sup>49</sup> Humans respond to flattery and criticism from computers,<sup>50</sup> and rate their experiences with

<sup>43</sup> See D. GARLAN et al., “Project Aura: Toward Distraction-Free Pervasive Computing,” IEEE Pervasive Computing, vol. 01, no. 2, pp. 22-31, Apr-Jun, 2002.

<sup>44</sup> See [http://en.wikipedia.org/wiki/Microsoft\\_Bob](http://en.wikipedia.org/wiki/Microsoft_Bob) (describing Microsoft’s unpopular virtual helper).

<sup>45</sup> *Id.*, p. 277.

<sup>46</sup> *Id.*, p. 8.

<sup>47</sup> B. REEVES and C. NASS, *The Media Equation: How People Treat Computers, Television, and New Media Like Real People and Places*, New York, Cambridge University Press, 1996.

<sup>48</sup> *Id.*, p. 14.

<sup>49</sup> *Id.*, p. 24.

<sup>50</sup> *Ibid.* (Chapters 2, 4).

computers more highly if the computer has a similar ‘personality’ (e.g., submissive) to their own.<sup>51</sup> The results applied to people of all ages and of diverse backgrounds, including those with a familiarity with technology.<sup>52</sup>

Further data around human-technology interaction suggests that the more human-like the medium, the greater the response. Canvassing the literature on human interaction with androids—i.e., “artificial system[s] designed with the ultimate goal of being indistinguishable from humans in its external appearance and behavior”<sup>53</sup>—informatics professors Karl MacDorman and Hiroshi Ishiguro conclude that “[h]umanlike appearance and behavior are required to elicit the sorts of responses that people typically direct toward one another”,<sup>54</sup> and that “the more humanlike the robot, the more human-directed (largely subconscious) expectations are elicited”.<sup>55</sup> In one cited study, test subjects exhibited greater unconscious eye contact behaviors (fixating on the right eye, typical of human-human interaction) when engaging with more humanoid robots.<sup>56</sup> In another, Japanese subjects only averted their gaze (a sign of respect) when engaging with the most human-like machines.<sup>57</sup> MacDorman and Ishiguro further offer several anecdotal examples of disparate treatment of robots. For instance, visitors to Ishiguro’s lab could be convinced to treat more mechanical robots roughly, but show respect toward Uando, a robot with an enhanced “aura of human presence,” due to automated response such as “shifting posture, blinking, and breathing”.<sup>58</sup> One visitor reportedly asked his wife’s permission before touching a ‘female’ robot.<sup>59</sup>

Importantly, research also shows that this tendency to anthropomorphise social media can also recreate in humans the sense of being observed. Thus, Terry Burnham and Brian Hare of Harvard University subjected 96 volunteers to a game in which they anonymously donate money or

---

<sup>51</sup> *Ibid.* (Chapter 8).

<sup>52</sup> *Id.*, p. 252.

<sup>53</sup> K. MACDORMAN and H. ISHIGURO, “The uncanny advantage of using androids in cognitive and social science research,” *Interaction Studies* 7:3, 2006, pp. 298-99.

<sup>54</sup> *Id.*, p. 316

<sup>55</sup> *Id.*, p. 309. There is an apparent point of similarity, often referred to as the “uncanny valley,” at which humans can become repulsed by an android. Many theories exist to explain this phenomenon, including that almost human androids create certain expectations that they necessarily violate (in that they are not perfect replicas). *Id.*, p. 299.

<sup>56</sup> *Id.*, p. 316.

<sup>57</sup> *Id.*

<sup>58</sup> *Id.*, pp. 313-14.

<sup>59</sup> *Id.*, p. 317.

withhold it. Where players were faced with a mere photo of Kismet—the robot designed by Cynthia Breazeal to elicit a social reaction in humans—they gave considerably more than those who were not.<sup>60</sup> In another experiment involving donation, subjects consistently donated more where the computer terminal they were using had eyespots on its screen.<sup>61</sup> In yet another study published in *Biology Letters*, UK psychologists found that the presence of a picture with eyes above a collection bin led people to pay for coffee on the honor system far more often than the presence of a picture of flowers.<sup>62</sup>

The standard explanation for this set of phenomena is that humans evolved at a time when representation was largely impossible, such that what appeared to be real was real in fact. As Reeves and Nass explain, “people are not evolved to twentieth-century technology. The human brain evolved in a world in which *only* humans exhibited rich social behaviors, and a world in which *all* perceived objects were real objects”.<sup>63</sup> In evolutionary terms, we are not much further along than our oldest ancestors.

American cognitive science professor H.R. Ekbia puts it slightly differently: humans as highly social animals have developed an innate ability to identify with other humans. This confers a tremendous survival advantage in that it tends to foster cooperation. The ability is often indiscriminate, however, with the result that humans often unconsciously attribute human emotions to objects or animals. Ekbia adds: “The AI community has, often inadvertently, taken advantage of this human tendency, turning what could be called innocent anthropomorphism to a professional and often unjustified, technoscientific one”.<sup>64</sup> That is, Ekbia believes that practitioners of AI have sometimes relied on the ELIZA effect to gloss over the difficulty in programming truly fulsome intelligent or social interactions.

#### IV. THE PRIVACY THREATS POSED BY SOCIAL AI

##### I. *Old paradigm: AI as active gatherers of information*

We have seen that social machines are on the rise and that humans treat

<sup>60</sup> V. WOODS, “Pay Up, You Are Being Watched,” *New Scientist*, Mar. 18, 2005 (reporting a 30% increase in giving when faced with Kismet).

<sup>61</sup> O. JOHNSON, “Feel the Eyes Upon You,” *N.Y. Times*, Aug. 3, 2008.

<sup>62</sup> M. BATESON et al., “Cues of Being Watched Enhance Cooperation in a Real-World Setting,” *Biology Letters*, 2(3), Sept. 22, 2006, pp. 412–14.

<sup>63</sup> B. REEVES and C. NASS, *The Media Equation*, p. 12 (emphasis in original).

<sup>64</sup> H.R. EKBIA, *Artificial Dreams*, p. 310.

social machines as though there were truly people. One application of this insight is to free computers from their historically hidden or passive role within surveillance and set machines to the active, interpersonal task of gathering of information. B.J. Fogg is a Stanford researcher who coined the term “captology”—“an acronym based on the phrase computers as persuasive technologies”.<sup>65</sup> In his 2003 book *Persuasive Technology: Using Computers to Change What We Think And Do*, Fogg details some of the techniques of captology, many of which consist of embedding physical, psychological, and social cues in computer interfaces for a variety of purposes. It turns out that one of the primary applications of persuasive technology has been information gathering.

Building on the work of Reeves, Nass, and others, Fogg directly compares mechanical persuaders to persuasive people. He explains certain advantages thoughtfully modeled computers will typically have. Computers can be more persistent than humans, in that humans tire and respond to social cues such as anger and shame.<sup>66</sup> Machines have no necessary form or clear identity, and can therefore facilitate anonymous persuasion. Computers can also “store, access, and manipulate huge volumes of data”. They can leverage a variety of “modalities,” beyond speech and body language. Computers can “scale,” in the sense of reaching millions of people at once. Similarly, computers can go where ordinary human strangers cannot—reaching into the home, a bathroom, or even a person’s clothing.

Fogg also details the dangers of persuasion by computer—some of which overlap his advantages. He identifies six “unique ethical concerns related to persuasive technology”.<sup>67</sup> First, he notes that a technology’s novelty can mask its persuasive intent. Humans may not be ‘on alert’ to an agenda in a neat new gadget. Second, computers have a positive reputation as credible and unbiased; this reputation can be exploited to hide a persuasive intent. Third, unlike sales people, computers do not tire; they can reach thousands simultaneously and persistently. Computers also control all “interactive possibilities”, i.e., the computer decides what happens next and what the user can see or do. Fifth, computers “can affect emotions but can’t be affected by them”.<sup>68</sup> Programmers can expect a social reaction from humans but can control the reaction of the persuasive technology that elicits it. Finally, computers are not “ethical agents”, in the sense that

---

<sup>65</sup> P.J. FOGG, *Persuasive Technologies*, p. xxv.

<sup>66</sup> *Ibid.*

<sup>67</sup> *Id.*, p. 213.

<sup>68</sup> *Id.*

they cannot take responsibility for an error.<sup>69</sup>

The gist of captology, then, is that computers and robots can be pressed into the task of persuading humans to engage in or refrain from behaviors through both direct and subtle social methods. This task has so far mostly involved gathering information. Canadian legal scholar Ian Kerr has explored the use of virtual representatives and other online “bots” that leverage techniques of AI and human-computer interaction in order to establish trust with, gather information about, and ultimately influence consumers.<sup>70</sup> In an insightful 2004 law review article Kerr asks, “What if bots could be programmed to infiltrate people’s homes and lives *en masse*, befriending children and teens, influencing lonely seniors, or harassing confused individuals until they finally agree to services that they otherwise would not have choose?”<sup>71</sup> The question proves a set up: Kerr observes that “[m]ost such tasks can be achieved with today’s bot technologies”.<sup>72</sup>

Kerr goes on to detail several “interactive agents” operating on the Web since 2000. One such agent is ELLEgirlBuddy, a text-based virtual representative for ELLEgirl.com that operates over instant messenger (“IM”). As Kerr explains: “ELLEgirlBuddy is programmed to answer questions about her virtual persona’s family, school life and her future aspirations, occasionally throwing in a suggestion or two about reading ELLEgirl magazine.” Although she has no actual body, she sometimes writes about her body image problems. Although she is in actuality only a few years old, ELLEgirlBuddy purports to be sixteen and seeks to replicate the lingo of a teenager, complete with emoticons.<sup>73</sup>

Among ELLEgirlBuddy’s most alarming functions is straightforward data collection. Every single response the bot receives or elicits is recorded—in all, millions of conversations over IM. This information is used in turn to further deepen the bond—and therefore trust—between the bot and its interlocutor.<sup>74</sup> (In social robotic parlance, ELLEgirlBuddy is an “expressive robot that respond[s] to people” and, when people treat it like the teen it purports to be, the robot learns from that.) Kerr points that the data has other, commercial value in that it could be used to target

---

<sup>69</sup> *Id.*, pp. 213–220.

<sup>70</sup> I. KERR, “Bots, Babes,” *o.c.*

<sup>71</sup> *Id.*, p. 312.

<sup>72</sup> *Id.*

<sup>73</sup> Emoticons are faces drawn with text. ;o)

<sup>74</sup> I. KERR, “Bots, Babes,” p. 316 (“In other words, these companies are constantly collecting incoming data from users and strong that information for the purposes of future interactions.”)

advertisements.<sup>75</sup>

The use of virtual personalities is not limited to the private sector. The U.S. Army has deployed an interactive virtual representative for its recruitment website.<sup>76</sup> The program, SGT Star,<sup>77</sup> appears as an avatar. He speaks out loud in addition to displaying text. He can act both funny and agitated, as when in response to a command to do pushups he yells: “Hey, I’m the sergeant, here, YOU drop down and give me twenty! I CAN’T HEAR YOU!!! COUNT ‘EM!!!” He can also take a compliment; if you tell SGT Star that you like him, he responds: “Thanks, I try”.

SGT Star purported function is to engage with users of the GoArmy website in order to answer questions and to provide other guidance such as the location of forms or local recruitment offices. Yet SGT Star also gathers information. As an initial matter, SGT Star prompts the user for his or her name before beginning the chat session. Moreover, the website invites users to sign in and provide more information (e.g., date of birth, address) for a more “personalised” SGT Star experience. SGT Star even invites users to “Tell A Friend” about him by submitting a name and email address, which will cause SGT Star to generate an email invitation to start a chat session with a third party.

According to the GoArmy privacy policy (in general a notoriously under-read document<sup>78</sup>), the Army records everything anyone says to SGT Star. The Army reserves the right to use all information gathered SGT Star for recruiting purposes, and to disclose such information as required by law.<sup>79</sup> The Army may therefore use chat transcripts in the aggregate to improve SGT Star’s ‘social skills’, or to identify particularly promising candidates for eventual follow up by a human recruiter. It remains largely unclear, however, whether the Army might use a SGT Star chat transcript to reject a candidate—for instance, by discovering the sexual orientation of a potential recruit on the basis of questions he asked about Army policy toward gays—a question he might not ask of a human recruiter.<sup>80</sup>

---

<sup>75</sup> *Id.*

<sup>76</sup> See <http://www.goarmy.com/ChatWithStar.do>.

<sup>77</sup> The SGT stands for “strong, trained, and ready.” *Id.*

<sup>78</sup> See, e.g., E. MORPHY, “Consumers Trust Brands, Not Policies,” CIO Today, Jan. 29, 2004 (citing research at Michigan State University).

<sup>79</sup> If you ask SGT Star about privacy, he responds: “I keep a record of all the chats I have with GoArmy users. My conversations are reviewed to ensure all potential recruits are getting the information that they need. However, your information will not be shared with the public.”

<sup>80</sup> The U.S. Army uses a “don’t ask, don’t tell” approach wherein gays may serve as long as they do not self-reveal their orientation. See 10 U.S.C. Sec. 654.

In short, through a combination of powerful processing and sophisticated social mimicry, it appears possible for companies and other institutions to collect information from individuals beyond that which even a large human work force could accomplish. As in the context of data mining, a computer equipped with artificial intelligence is capable of engaging thousands of individuals simultaneously, twenty-four hours a day. But here the agent is able to leverage the power of computers to persuade via carefully orchestrated social tactics known to elicit responses in humans. In an age of national security and targeted advertising, citizen and consumer information is at an all time premium.<sup>81</sup> Techniques of AI and HCI create the opportunity for institutions to leverage the human tendency to anthropomorphise and other advantages computers hold over humans (ubiquity, diligence, trust, memory, etc.) to facilitate and otherwise impracticable depth and breadth of data collection.

## 2. *New paradigm: social AI as subject*

We have seen various applications of AI that threaten privacy by substituting a machine or software function for a human task, thereby augmenting the human power to observe. Thus, AI can listen to phone conversations so that a human does not have to, comb through video or other data better and faster than a human, or be sent out to recruit or inquire on behalf of an organization using much of the social leverage of a real person, but with none of the limitations. Yet given the power of social AI to signal the presence of a human, the distribution of social machines may have still deeper, if unintended, impacts on privacy.

As an initial matter, the appearance of social AI in historically private spaces may lessen the opportunity for solitude and free reflection. Many privacy theorists have expounded upon the importance of private space, wherein one can “be themselves” and even transgress otherwise oppressive social norms. As Alan Westin famously writes in his 1970 treatise on privacy, *Privacy and Freedom*: “There have to moments ‘off stage’ when the individual can be ‘himself; tender, angry, irritable, lustful, or dream filled. ... To be always ‘on’ would destroy the human organism”.<sup>82</sup> Westin further cites the “need of individuals for respite from the emotional stimulation of daily life. ... [T]he whirlpool of active life must lead to some quiet water, if only so that the appetite can be whetted for renewed social engagement.”<sup>83</sup>

---

<sup>81</sup> See, e.g., A. MCCLURG, “A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 Nw. U. L. Rev. 63 (2003) (discussing institutional data demand and data mining trends).

<sup>82</sup> A. WESTIN, *Privacy and Freedom*, New York, Anthem 1970, p. 35.

<sup>83</sup> *Id.*

According to Westin, “[p]rivacy provides the change of pace that makes life worth savoring”.<sup>84</sup> For Westin, privacy protects “minor non-compliance with social norms” that “society really expects many persons to break”, and the important opportunity to “deviate temporarily from social etiquette”.<sup>85</sup>

Many other scholars have explored the same line of thought. In the words of political theorist Hannah Arendt, “[a] life spent entirely in public, in the presence of others, becomes ... shallow. ... A space apart from others has enabled people to develop artistic, political, and religious ideas that have had lasting influence and value when later introduced into the public sphere”.<sup>86</sup> American law scholar Paul Schwartz argues that the belief that one is being constantly observed interferes with self-determination.<sup>87</sup> Julie Cohn argues similarly that “pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream”.<sup>88</sup> According to prolific privacy scholar Daniel Solove, “[n]ot only can direct awareness of surveillance make a person feel extremely uncomfortable, but it can also alter her behavior. Surveillance can lead to self-censorship and inhibition”. Solove further notes that “[e]ven surveillance of legal activities can inhibit people from engaging in them”.<sup>89</sup>

If, as many contend, safeguarding occasional solitude is a central goal of privacy law, social AI may bypass existing protections by introducing the appearance and feeling of a human in an unlimited array of contexts. Consider just a few examples: Japanese software company MetaboInfo makes a virtual wife that appears on your cell phone and reminds you of chores;<sup>90</sup> an exhibit of a future house by Disney showcases a mirror that sees you and suggests outfits;<sup>91</sup> the Figera vacuum approaches its owner and responds to voice commands;<sup>92</sup> experiments are being conducted around whether placing robots or voice-interface computers in cars can stop road rage; etc.<sup>93</sup> As captology expert BJ Fogg explains, “computing

---

<sup>84</sup> *Id.*

<sup>85</sup> *Id.*

<sup>86</sup> D. SOLOVE, “A Taxonomy of Privacy,” pp. 554-55.

<sup>87</sup> *Id.*, p. 494.

<sup>88</sup> *Id.*

<sup>89</sup> D. SOLOVE, “‘I’ve Got Nothing To Hide’ and Other Misunderstandings of Privacy,” 44 San Diego L. Rev. 745 (2007), p. 267.

<sup>90</sup> See <http://www.metaboinfo.com/okusama/> (website in Japanese).

<sup>91</sup> P.J. O’RORKE, “Future Shlock,” *The Atlantic*, Dec. 2008.

<sup>92</sup> See <http://gizmodo.com/5105633/the-figura-vacuum-bot-allows-you-to-boss-it-around>.

<sup>93</sup> T.E. GALOVSKI and E.B. BLANCHARD, “Road rage: A domain for psychological intervention?”, *Aggression and Violent Behavior*, 2004, No 9, pp. 105—127.

applications are becoming commonplace in locations where human persuaders would not be welcome, such as bathrooms and bedrooms, or where humans cannot go (inside clothing, embedded in automotive systems, or implanted in a toothbrush).<sup>94</sup>

Social AI may also impact personal privacy in the aggregate, by creating unease around the massive computer custodianship of human data. Hardly any aspect of human life today remains untouched by computers; this trend will only grow as computer become embedded into our streets, walls, and even our clothing. Meanwhile, the public sense of computer intelligence and evaluative capabilities—fueled by our tendency to anthropomorphise, by the rise in prominence of tech media coverage, and by claims of competitive practitioners—continues to develop. This synergy could, in theory, lead to widespread and intractable discomfort with computer information custodianship.

Artificial intelligence has clearly seen its share of breakthroughs throughout its history, many of which have been widely reported by the media.<sup>95</sup> The field stands poised to make many more. In part by leveraging well-understood AI tactics and incredible but steady gains in computational power, projects such as the Defense Advanced Research Agency (DARPA)'s "Cognitive Agent that Learns and Organises" are making notable strides in advancing computer learning, and setting ambitious but attainable long-term goals.<sup>96</sup>

Indeed, computer and robotics insiders publicly predict that machines will be as or more intelligent than humans within a few decades. Jim Gray of Microsoft Research has speculated that computers will pass the famous Turing Test—i.e., the test of machine intelligence devised by Alan Turing wherein a machine must fool a trained expert into believing it is human—by

---

<sup>94</sup> P.J. FOGG, *Pervasive Computing*, at p. 10.

<sup>95</sup> See, e.g., [http://www.sciencedaily.com/news/computers\\_math/artificial\\_intelligence/](http://www.sciencedaily.com/news/computers_math/artificial_intelligence/) (compiling artificial intelligence headlines); <http://ai-depot.com/news/> (same); <http://www.aaai.org/AITopics/pmwiki/pmwiki.php/AITopics/AINews> (same).

<sup>96</sup> R. BRACHMAN and Z. LENIOS, "DARPA's New Cognitive Systems Vision," *Computing Research News*, Vol. 14/No. 5, pp. 1, 8. (Nov. 2002):

A cognitive computer system should be able to learn from its experience, as well as by being advised. It should be able to explain what it was doing and why it was doing it, and to recover from mental blind alleys. It should be able to reflect on what goes wrong when an anomaly occurs, and anticipate such occurrences in the future. It should be able to reconfigure itself in response to environmental changes. And it should be able to be configured, maintained, and operated by non-experts.

the middle of this century.<sup>97</sup> A German software program competing in the International Turing Competition managed recently to fool three of twelve judges into believe it was a person.<sup>98</sup> Speaking as a keynote at a large technology conference, Justin Ratner, Intel's chief technology officer, observed in August 2008:

The industry has taken much greater strides than anyone ever imagined 40 years ago. There is speculation that we may be approaching an inflection point where the rate of technology advancements is accelerating at an exponential rate, and machines could even overtake humans in their ability to reason, in the not so distant future.<sup>99</sup>

According to a recent report, the manager of the Adaptive Systems group at Microsoft estimated that "about a quarter of all Microsoft research is focused on AI efforts".<sup>100</sup> Google founders Sergey Brin and Larry Page have repeatedly articulated their goal of creating "obviously artificial intelligence", in the sense of a truly "smart" program that "understands" user queries and the universe of potential results to the point that searches as well as a human with immediate access to most of the Internet.<sup>101</sup>

Clearly the impact of "strong" artificial intelligence—in the John Searle sense of actual self-awareness—would be profound across all sectors.<sup>102</sup> Predictions of strong AI have fallen flat before, however, and many within

---

<sup>97</sup> *Id.*, p. 501. See also *id.*, p. 460 (robotics pioneer Hans Moravec predicting strong AI by 2030).

<sup>98</sup> WILL PAVIA, "Machine takes on man at mass Turing Test," Times Online (Oct. 13, 2008), available online at [http://technology.timesonline.co.uk/tol/news/tech\\_and\\_web/article4934858.ece](http://technology.timesonline.co.uk/tol/news/tech_and_web/article4934858.ece).

<sup>99</sup> Intel News Release, Aug. 21, 2008, available online at <http://www.intel.com/pressroom/archive/releases/20080821comp.htm?cid=rss-90004-CI-211570>.

<sup>100</sup> J. GASKIN, "Whatever Happened to Artificial Intelligence?," Network World, Jul. 23, 2008 (emphasis added).

<sup>101</sup> See <http://ignoranceisfutile.wordpress.com/2008/09/13/google-founders-artificial-intelligence-quotes-archive/> (collecting AI quotes from Google principals). Brin reportedly said the following in November of 2002: "Hal could... had a lot of information, could piece it together, could rationalise it. Now, hopefully, it would never... it would never have a bug like Hal did where he killed the occupants of the space ship. But that's what we're striving for, and I think we've made it a part of the way there." *Id.*

<sup>102</sup> See L. SLOCUM, "Legal Personhood for Artificial Intelligence," 70 N.C. L. Rev. 1231 (1992) (discussing whether AI could serve as a trustee); *id.* (discussing John Searle). See also C. STONE, "Should Trees Have Standing? Toward Legal Rights for Natural Objects," 45 Cal. L. Rev. 450, 453-57 (1972) (discussing whether AI could have standing).

the field argue that humans may never recreate actual intelligence.<sup>103</sup> This particularly achievement is at a minimum decades away. A potentially more interesting question in the short run (i.e., the next five to ten years) is whether computers will reach a level of sophistication at which humans become unsure of the AI's intelligence and, consequently, *uncomfortable* with their extensive 'knowledge'.

Today, humans appear to trust computers and computer servers with their personal information. The prevailing view of computers remains the desktop—a complex but lifeless automaton that manipulates data without interest.<sup>104</sup> Thus, in seeking to allay fears over its practice of scanning web-based email messages in order to display contextual advertisements, the Internet giant Google is careful to represent that the scanning is conducted by a computer. “Google does NOT read your email... Gmail [or Google Mail] is a technology-based program, so advertising and related information are shown using a completely automated process”.<sup>105</sup>

In the context of national security, American thought leaders debate whether machine shifting through public and private data can amount to a government invasion. Judge and scholar Richard Posner argues that “[m]achine collection and processing of data cannot, as such, invade privacy”, such that computer data access or citizen surveillance does not in and of itself trigger a search or seizure for purpose of the Fourth Amendment.<sup>106</sup> Prosecutor turned legal scholar Orin Kerr also holds that no search occurs until “information from or about the data is exposed to human observation,” not when it is simply “processed by a computer”.<sup>107</sup> Law professor Larry Lessig also uses the example of a search by a government computer program that mindlessly borrows through citizen data (a so-called “worm”) to test the parameters of search and seizure law in cyberspace.<sup>108</sup>

This image of a passive conduit may change, however, if and when computers reach a threshold of apparent intelligence wherein processing

<sup>103</sup> See S. RUSSELL and P. NORVIG, *Artificial Intelligence*, pp. 947-60 (canvassing the literature).

<sup>104</sup> It is precisely this human view of computers as unbiased, trustworthy data processors that creates the opportunity for persuasion present in captology. B.J. FOGG, *Persuasive Technologies*.

<sup>105</sup> See <http://mail.google.com/support/bin/answer.py?answer=6599&topic=12787>.

<sup>106</sup> R. POSNER, “Our Domestic Intelligence Crisis,” *The Washington Post*, Dec. 21, 2005.

<sup>107</sup> O. KERR, “Searches and Seizures in a Digital World,” 119 *Harv. L. Rev.* 531, 551 (2005).

<sup>108</sup> L. LESSIG, *Code 2.0*, New York, Basic Books, 2006, pp. 20-23.

begins overly to resemble human judgment. Given a handful of factors—namely, the human tendency to anthropomorphise discussed in detail above, the aggressive claims of AI practitioners and critics, the occasional hyperbole of the media, and the lack of any definitive test of intelligence—humans could come to equate computer mentality with human mentality in the relatively near term. This in turn could lead to an uncomfortable reexamination of computers as passive custodians of consumer and citizen data.<sup>109</sup>

## V. THE (IN)ADEQUACY OF U.S. PRIVACY LAW

American privacy law already contains the seeds of a solution to many of the emerging privacy harms identified in this essay. A notorious patchwork, American privacy law nevertheless requires notice about the collection, use, and disclosure of personal and other information<sup>110</sup> and is relatively steadfast in its protection against invasions into private space without adequate process.<sup>111</sup>

The privacy community has already begun to propose concrete solutions to perceived abuses of sophisticated and widespread data mining by government and industry. Andrew McClurg argues, for instance, for a resuscitation of the U.S. common law tort of appropriation (discussed by Warren and Brandeis in *The Right to Privacy*<sup>112</sup>) as a response to the creation and use of consumer profiles.<sup>113</sup> Appropriation refers to the use of another's identity—generally, their name or “likeness”—to one's own benefit without consent. Such a use can amount to an invasion of privacy under American common law.<sup>114</sup> McClurg argues convincingly that the digital

---

<sup>109</sup> Changes to user interfaces may have more immediate effects, however, in the realm of voice-driven search. In a recent interview, Google's vice president for search Marissa Mayer discussed the hope that, within a few years, users might be able to interact with Google orally by “asking questions by voice.” See <http://www.techcrunch.com/2008/12/10/marissa-mayer-at-le-web-the-almost-complete-interview/>. Query whether individuals will search for the same things when it feels to the user that they are speaking with a person.

<sup>110</sup> See, e.g., California Online Privacy Protection Act of 2003, Bus. & Prof. Code Sec. 22575-22579 (California statute requiring companies that collect personal information to link to a privacy policy). The FTC also holds companies to their claims about data and sets minimum thresholds of notice for material changes to policy. See, e.g., *In the Matter of Gateway Learning Corp.*, FTC File No. 042-3047 (2004).

<sup>111</sup> D. SOLOVE, “A Taxonomy of Privacy,” 154 U. Pa. L. Rev. 477 (2006), p. 552 (“For hundreds of years, the law has strongly guarded the privacy of the home.”).

<sup>112</sup> S. WARREN AND L. BRANDEIS, “The Right to Privacy,” 4 Harv. L. Rev. 193 (1890).

<sup>113</sup> A. MCCLURG, “A Thousand Words are Worth a Picture.”

<sup>114</sup> See Restatement (Second) of Torts Sec. 652C (1977).

profile that results from sophisticated data mining constitutes an “inner identity” that can trigger the tort.

American law professor Daniel Solove also urges a more comprehensive understanding of privacy law that encompasses the “Kafkaesque” nature of modern surveillance<sup>115</sup> and has shown how to arrive at an appropriate balance between security interests and privacy rights by meticulously cataloguing the harms of data mining. Digital rights groups such as the San Francisco based Electronic Frontier Foundation have brought suit against telephone providers and the government itself in an effort to understand and domesticate government data mining.<sup>116</sup>

Similarly, the use of social media to persuade consumers to give up information or to purchase particular products has a ready analog in tactics already being investigated by national and local consumer protection agencies. In the United States, Section 5 of the FTC Act prohibits “unfair or deceptive trade practices,” broadly defined.<sup>117</sup> The Federal Trade Commission is charged with enacting and enforcing policy aimed at prohibiting unfair, deceptive, or anti-competitive practices within the industries in its jurisdiction. The agency has turned its attention in recent years to online data collection practices such as the traffic of users’ surfing habits,<sup>118</sup> as well as the use of ‘buzz’ or subliminal marketing wherein products are promoted without notice that the speaker is affiliated with an advertising company. State attorneys general have also investigated online information gathering practices and, in cases, reached agreements with companies perceived to gather or use data too aggressively.<sup>119</sup> Ian Kerr explains that the use of AI bots particularly for marketing and consumer information gathering may violate similar Canadian consumer protection

---

<sup>115</sup> D. SOLOVE, “‘I’ve Got Nothing To Hide,’” p. 756.

<sup>116</sup> See EFF Press Release, “EFF Sues NSA, President Bush, and Vice President Cheney to Stop Illegal Surveillance,” Sept. 18, 2008, available online at <http://www.eff.org/press/archives/2008/09/17-0>.

<sup>117</sup> Federal Trade Commission Act, 15 U.S.C. Secs. 41-58, as amended.

<sup>118</sup> FTC Press Release, “FTC Staff Proposes Online Behavioral Advertising Privacy Principles,” Dec. 20, 2007, available online at <http://www.ftc.gov/opa/2007/12/principles.shtm>.

<sup>119</sup> Online advertising company DoubleClick entered into a consent decree with a coalition of state attorneys general in 2001, agreeing not to combine certain categories of information following a merger with offline consumer profiler Abacus. See, e.g., Washington State Office of the Attorney General Press Release, “States Settle with DoubleClick,” April 2001, available online at <http://www.atg.wa.gov/pressrelease.aspx?id=5848>.

regulations.<sup>120</sup>

In other cases, however, the law may have no obvious starting point in addressing these emerging privacy harms. As discussed above, the effect of social media is often a direct but subconscious one. It is not that humans will use a technology to invade one another's privacy; rather, the object will be treated as itself human. The danger is that voice-driven, natural language interfaces will become the norm; that computers will increasingly be endowed with personalities; and that robots with anthropomorphic features will come to be voluntarily accepted as a daily part of life (as is increasingly the case in Japan). Simultaneously, but at an examined level, privacy will be eroded by the subconscious perception that we are always being watched and evaluated.

An extreme example with intentional and obvious chilling effects on speech, such as a holographic police officer that follows around each citizen, could in theory trigger the First Amendment of the U.S. Constitution.<sup>121</sup> But there may be no immediate legal solution to a diffuse introduction of social media into private space by natural means. Similarly, the discomfort we may begin to feel at AI custodianship of data may not be reducible to a legally cognizable injury. Although real anxiety could result, perhaps little more can be said about AI capable of extremely accurate judgments or vested with the appearance of common sense is that it is 'creepy'. American privacy law may be ill-suited to protect against such subtle and (for now) speculative harms.<sup>122</sup>

Solutions may ultimately come from outside of privacy law. It turns out that in other contexts, American law forces consideration of subjective interests such as fear or discomfort. Thus, for instance, in the (pun-ridden) case of *Stambovsky v. Ackely*, a New York appeals court recognised a buyer's right to rescind purchase of a home after he learned that it was haunted by a poltergeist.<sup>123</sup> It was no reply that poltergeists do not exist. The buyer could not be forced to live with a ghost merely because the

---

<sup>120</sup> I. KERR, "Bots, Babes," at p. 321 ("The fair information practices set out in Appendix 2 of the Canadian Code contain a number of requirements that are clearly not respected by ActiveBuddy and many other bot-based business models.").

<sup>121</sup> *Cf. Laird v. Tatum*, 408 U.S. 1, 11 (1972) ("In recent years this Court has found in a number of cases that constitutional violations may arise from the deterrent, or 'chilling,' effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights.").

<sup>122</sup> D. SOLOVE, "A Taxonomy of Privacy," p. 562-63 ("Too many courts and policymakers struggle even identifying the presence of privacy problems. . . . Unfortunately, due to conceptual confusion, courts and legislatures often fail to recognise privacy problems . . .").

<sup>123</sup> 169 A.D. 2d 254 (N.Y. Ct. App. 1991).

existence of ghosts has not been established.<sup>124</sup> Sellers and brokers must also disclose other stigmas such the occurrence in a home of a multiple murder.<sup>125</sup> In the context of pollution, litigants have pursued a variety of harms bred of unrealised fears.<sup>126</sup> Accordingly, one can imagine a requirement that an entity disclose that it is using sophisticated AI and offer to store user information separately.

Another useful analog might be the requirement of warning labels for non-obvious product defects. The Food and Drug Administration and individual states often require harmful goods to contain warnings as to their contents, and the existence of a warning label can sometimes provide a meaningful defense against a civil action for product liability. Where a car comes equipped with an active AI passenger, for instance, its user manual could warn that humans react to social machines as though they were truly humans, and that constantly being in the presence of others can lead to discomfort.

Viable solutions are equally likely to come from outside the law, especially in the short term. They might include the inclusion of privacy in ethics discussions around social media, the participation of developers of AI in efforts to build privacy protections into emerging technology,<sup>127</sup> and sustained efforts at public education by industry and government.<sup>128</sup> In his aforementioned book on captology, Fogg creates a framework by which to assess the ethical implications of a given instance of persuasive technology. He concludes that:

Ultimately, education is the key to more ethical persuasive

---

<sup>124</sup> In *Stambovsky*, the tongue-in-cheek court actually held the house to be haunted “as a matter of law.” *Id.*

<sup>125</sup> See *Reed v. King*, 145 Cal. App. 3d 261 (1983) (holding that plaintiff stated a cause of action for defendant-broker’s failure to disclose that house was site of multiple murder).

<sup>126</sup> See, e.g., *City of Santa Fe v. Komis*, 845 P.2d 753, 757 (N.M.1992) (awarding land owner damages due to fear of nuclear waste); *Lunda v. Matthews*, 613 P.2d 63, 67-68 (Or.Ct.App.1980) (allowing emotional distress damages for fear of air emissions from cement plant); *Heddin v. Delhi Gas Pipeline Co.*, 522 S.W.2d 886, 888 (Tex.1975) (awarding damages to landowner due to fear that pipeline on adjoining land would explode); *Texas Elec. Serv. Co. v. Nelon*, 546 S.W.2d 864, 871 (Tex.Civ.App.1977) (allowing landowner to recover for fear of nuclear waste transported nearby).

<sup>127</sup> UK’s Information Commissioner’s Office has, for instance, commission the Enterprise Privacy Group to produce a new report on the impact on personal privacy of various activities across multiple industries. Applications of social AI should be included in such a report.

<sup>128</sup> See also T. ZARSKY, “Mine Your Own Business!,” Sec. III (discussing the role of public education in addressing AI data mining techniques).

technologies. Designers and distributors who understand the ethical issues ... will be in a better position to create and sell ethical persuasive technology products. Technology users will be better positioned to recognise when computer products are applying unethical or questionably ethical tactics to persuade them.<sup>129</sup>

Calling attention to and discussing these phenomena is a necessary first step to heading off or addressing a novel set of privacy threats.

## VI. CONCLUSION

Our conception of what constitutes an invasion of personal privacy continues to evolve—over time, dramatically. Consider the origin of the term “Peeping Tom.” Tom was an adolescent with the bad luck to be within the city limits of Coventry when Lady Godiva made her (in)famous naked ride to protest taxes. Unlike other young men, Tom openly gawked at Lady Godiva’s naked form as she passed. Today, were a young man *not* to gawk at naked woman on a horse, we might be amazed. We would certainly give no credence to a complaint by or on behalf of the naked woman. (We would say that she willingly exposed herself in public where she has no expectation of privacy.) At the time of the legend, circa 1050, Tom was blinded for his impudence.<sup>130</sup>

Even as our privacy norms evolve, however, a set of basic biological facts remains constant: humans react to social media as though it were human.<sup>131</sup> This disconnect between the state of evolution and the state of our technology continues to be exploited—sometimes inadvertently—by developers of certain types of AI in order to develop machine intelligence, foster machine acceptability, and improve user experiences. As a consequence, humans may face a meaningful reduction in their already waning privacy. Upon a thorough canvass of the literature, German privacy theorist Beate Rössler concludes that “a person’s privacy can be defined, therefore, in these three ways: as illicit interference in one’s actions, as illicit surveillance, as illicit intrusions in rooms or dwellings”.<sup>132</sup> Particular techniques of artificial intelligence can be said to violate each of these definitions.

Clearly, artificial intelligence has led to important medical, commercial, and other benefits, and promises many more. And where AI merely

---

<sup>129</sup> P.J. FOGG, *Persuasive Technologies*, p. 235.

<sup>130</sup> D. SOLOVE, “A Taxonomy of Privacy,” p. 492.

<sup>131</sup> B. REEVES and C. NASS, *The Media Equation*.

<sup>132</sup> B. ROSSLER, *The Value of Privacy*, Cambridge, Polity Press, 2005, p. 9.

supports a human practice—as in the case of data mining or interviewing consumers—the law seems well-equipped to provide a meaningful solution. All that may be needed is to expand the law through ordinary methods to encompass and limit the underlying offensive activity. In other cases the solution is not as simple. More subtle and comprehensive changes may be required to mitigate the impact of sophisticated social agents in our midst. Ultimately, however, it may be that “we won’t know enough to regulate [AI] until we see what it actually looks like”.<sup>133</sup>

---

<sup>133</sup> J. MCCARTHY, “Problems and Projections in CS for the Next 49 Years,” *Journal of the ACM*, 2003.

# **PROPERTY IN PERSONAL DATA: A EUROPEAN PERSPECTIVE ON THE INSTRUMENTALIST THEORY OF PROPERTISATION**

Nadezda Purtova\*

## **I. BACKGROUND, RESEARCH QUESTION AND STRUCTURE OF THE PAPER**

Since early 1970s the US scholars have been ‘playing’ with the idea to introduce property rights in personal data.<sup>1</sup> Next to acknowledging already existing phenomenon of commodification of personal data, propertisation would potentially offer a solution to the data protection problem resulting from the Information Revolution. Introduction of property rights in personal data has been advocated from several perspectives: arguably it would help individuals reclaim lost control over their personal data, or acknowledge an inherent connection between an individual and data pertaining to him (natural rights theory).<sup>2</sup> Other commentators see benefits of propertisation in a rhetorical value of property talks.<sup>3</sup> Some believe that only propertisation is able to overcome inherent limitations of the US legal and political system.<sup>4</sup> The most discussed approaches to information privacy as property have been taken from the perspective of economic analysis of law.<sup>5</sup> Of a special interest is a part of the economic

---

\* PhD candidate at TILT - Tilburg Institute for Law.

<sup>1</sup> A. F. WESTIN, *Privacy and Freedom*. London, Sydney, Toronto, the Bodley Head, 1967. P. E. AGRE, M. ROTENBERG eds., *Technology and Privacy: the New Landscape*, Cambridge, MIT Press, 1997.

<sup>2</sup> D. J. SOLOVE, “Privacy and Power: Computer Databases and Metaphors for Information Privacy,” *Stanford Law Review*, 2001, No 53, p. 1393, at p. 1446 (although he does not develop the natural law argument further); V. BERGELSON, “It’s Personal, but Is It Mine? Toward Property Rights in Personal Information”, *U.C. Davis Law Review*, 2003, No 37, p. 379, at p. 430; M. J. RADIN, “Property and Personhood”, *Stanford Law Review*, 1982, No 34(5), pp. 957-1015, at p. 959.

<sup>3</sup> “Property talk is just how we talk about matters of great importance. [...] “If you could get people (in America, at this point in history) to see certain resource as property, then you are 90 percent to your protective goal.” (L. LESSIG, “Privacy as Property”, *Social Research: An International Quarterly of Social Sciences*, 2002, No 69(1), pp. 247-269.

<sup>4</sup> See J. LITMAN, “Information Privacy/Information Property”, *Stanford Law Review*, 2000, No 52, p. 1283.

<sup>5</sup> Although this is a simplification, when applied to the argument for propertisation, this article uses “utilitarian,” “economic,” and “instrumental” interchangeably;

argument, made among others by Lessig<sup>6</sup> who invokes property as a regulatory tool and an instrument to create a general, more effective system of data protection incorporating *inter alia* privacy enhancing technologies (PETs). This paper will refer to this argument as the instrumentalist theory of propertisation.

In brief, new developments in personal-data related practices both in Europe and the US have been generally attributed to several interconnected processes: emergence of the service economy, new marketing techniques, welfare state and recently, security concerns in the aftermath of 9/11 – all reinforced by technological developments.

In the circumstances of industrialisation businesses were striving to wear off detrimental consequences of mass production for the salesperson-customer relationship and tune their products and services more in accordance with customers' preferences. Targeted marketing has emerged as a solution largely based on linking demographic information to consumer behaviour and as a result giving rise to the interest in bulk quantities of those data to build a consumer profile. Simultaneously in public sector, state's functions expanded to the provision of welfare for the citizens on the grounds of family and employment status, health condition, etc. To exercise those obligations state, too, needed more personal information. The 9/11 events gave rise to major security concerns which were addressed by tremendous increase in surveillance practices and even more intensive (also secret) collection of information about (suspect groups of) individuals, data mining and profiling.

It became necessary for public agencies and private businesses alike to collect more information about individuals. These developments have resulted in both qualitative and quantitative growth of personal data collection which would not be possible without technology. Besides the fact that computers made processing of personal information faster, they also made storage of bulks of data and linking previously disintegrated records a reality and enabled data mining, profiling, and automated-processing based decision-making. Internet has provided a new and unique source of data. Along with the data routinely recorded as a result of every online transaction, the non-static nature of a web-page enables the data collectors to secretly track the way people browse the Internet (clickstream data). Internet made massive online social networking

---

<sup>6</sup> Cohen also speaks of law as only a mechanism to create incentives to build a general privacy infrastructure (see Cohen 2000, p. 1437-38). Cohen refers to Phil Agre who described 'technologies of identity' which made it possible to prevent collection of personal data (P. E. AGRE, M. ROTENBERG eds, *Technology and Privacy: the New Landscape*. Cambridge, MIT Press, 1997).

possible by means of which people knowingly disclose their personal information and (often unknowingly) make their data available for third parties commercial collection.<sup>7</sup>

Given profits personal information brings and costs its collection and processing require, marketers soon realized an opportunity to avoid the costs by buying the needed data from already existing databases of other enterprises.<sup>8</sup> A new branch of the information industry – the database builders – has emerged devoted to the collection of information, also via web-sites where people are offered to trade their personal data for goods, discounts, or services. A market of databases has emerged.<sup>9</sup> This process is also referred to as commodification of personal information.

Despite the fact that Europe faces similar challenges of the Information Revolution, including commodification of personal data,<sup>10</sup> so far only few European commentators have reflected on the possibility of propertisation.<sup>11</sup> This paper will try to fill in a small part of the gap and make some first tentative steps to answer the question whether the proposal to create a general system of data protection by introducing property rights is feasible in and/or compatible with the European legal system,<sup>12</sup> or, alternatively, if the instrumentalist theory of propertisation may be applied to Europe as well. The preliminary answer to this question is that it cannot.

With regard to the scope of the paper, three important remarks should be made. First, although “European” may have several alternative meanings, by European perspective on the idea of propertisation this research means the one unique for the framework of the European Union which is also

---

<sup>7</sup> A. ACQUISTI, R. GROSS, “Information Revelation and Privacy in Online Social Networks (The Facebook case)”, *ACM Workshop on Privacy in the Electronic Society (WPES)*, 2005.

<sup>8</sup> D.J. SOLOVE, *o.c.*, p. 1407.

<sup>9</sup> D.J. SOLOVE, *o.c.*, p. 1407.

<sup>10</sup> For an overview of personal data practices in the US see e.g. D.J. SOLOVE, *o.c.*. In Europe – L. A. BYGRAVE, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, The Hague, Kluwer Law International, 2002. On surveillance, data mining, and profiling in the context of security in Europe and the US see P. DE HERT, R. BELLANOVA, *Data protection from a Transatlantic Perspective: the EU and US move towards an International Data Protection Agreement?* Brussels, 2008.

<sup>11</sup> See, e.g. J. E. J. PRINS, “Property and Privacy: European Perspectives and the Commodification of our Identity”, *The Future of the Public Domain, Identifying the Commons in Information Law*, The Hague, Kluwer Law International, 2006, 16, pp. 223-257.

<sup>12</sup> By European legal system this paper will mean the legal system of the European Union.

bound by the law of the Council of Europe. Given that the EU legal system represents a coherent legal order, defining Europe as EU offers a much better chance of developing a coherent approach to the idea of propertisation. Second, present research limits itself to legal analysis and is not aimed at establishing or verifying any causal connections which are, in the author's opinion, a domain of the sociology of law. In other words, the paper will not examine whether the measures meant by propertisation will achieve the results they are argued to be able to achieve, or whether they will be more effective than alternative legal tools. That is, it is out of the scope of this paper whether application of Lessig's proposal actually leaves Europe with a 'better' system of protection of personal data. The final remark is that the paper is only the first attempt to sketch the roadmap of analysis of Lessig's idea of propertisation in the European context and is largely exploratory.

The argument against viability of Lessig's instrumentalist theory in Europe will be made in several steps. First, the paper will explain the very idea of Lessig's theory of propertisation of personal data as explained in the book *Code and Other Laws of Cyberspace*,<sup>13</sup> with a special emphasis on the economic notion of property it operates with. The conclusion will be made that economic analysis of law in general and as utilised by Lessig seems to put an equation between economic and common law concepts of property. Finally, Lessig's theory will be considered on its face and substance, *i.e.* two questions will be answered: whether without regard to the content of the property rights, propertisation in Europe is formally possible, and if yes, whether Lessig's scenario of propertisation in its substance is compatible with the reality of the European legal system. The conclusion will be made that although propertisation of personal data is a legal possibility, when executed in the European legal system it will not be able to fulfil the functions expected from it according to Lessig's theory.

## II. INSTRUMENTALIST DISCOURSE ON PROPERTISATION

Lessig's instrumentalist theory of propertisation is just one of at least three versions of the economic argument to introduce property rights in personal data.<sup>14</sup> The other two versions consider property as a tool enabling market exchange which, provided transaction costs are minimal, will achieve an optimal (*i.e.* efficient) level of privacy by balancing the value of personal information to a company against the value of the (non-

---

<sup>13</sup> L. LESSIG, *Code and Other Laws of Cyberspace*, New York, Basic Books, 1999.

<sup>14</sup> For a more detailed analysis of all three interpretations see N. PURTOVA, "Propertisation of Personal Data: Learning from American Discourse", forthcoming in *SCRIPT-ed*.

disclosure of) information to the individual and the larger social value of data protection.<sup>15</sup> Instrumentalist theory stands out since it is not concerned with efficiency but merely uses the logic of the economic analysis to propose the creation of an overall system of data protection which would comprise law, technology and market tools. Their interaction can ensure a proper level of information privacy.

In Lessig's theory, property is an engine bringing the general system of data protection into action. Lessig builds an economic argument that property rules would permit each individual to decide what information to disclose and protect "both those who value their privacy more ... and those who value it less."<sup>16</sup> First, he argues pretty traditionally, information privacy is in essence control over personal information. Second, unlike in the real world, the architecture (or "code") of a cyberspace makes collection of information difficult to spot, and control over that information – unrealistic to exercise for lay people. Third, such an architecture is a result of human activity and, therefore, can be altered.<sup>17</sup> Fourth, the US information processing practices are based on self-regulation, *i.e.* there is no general legislation requiring businesses to alter this architecture and use privacy-friendly technologies. Nor is there motivation to account for interests of the individuals. In absence of property interests, the companies make use of personal data for free. However, if individuals had property rights in personal data, it would force businesses to negotiate with the individuals, account for their interests, and alter the architecture, *i.e.* invest into development of PETs. The individual privacy would be better secured, not only by law but by interaction of the latter, market mechanisms and technologies.<sup>18</sup>

Lessig's argument operates with the reading of the legal concept of property given by Calabresi and Melamed<sup>19</sup> and adopted by the literature on economic analysis of law. Property is defined as the opposite of the liability rule. Both are the means invoked to protect a certain entitlement. When the entitlement is protected by a property rule, it cannot be taken

---

<sup>15</sup> Solove brings as examples of such an approach J. HAGEL III & M. SINGER, *Net Worth: Sharing Markets When Consumers Make the Rules*, 1999, pp. 19-20 (advocating for an "infomediary" between consumers and vendors who would broker information to companies in exchange for money and goods to the consumer); P. FARHI, "Me Inc: Getting the Goods on Consumers", *Washington Post*, 14 February 1999, at p. H1.

<sup>16</sup> L. LESSIG, *supra* note 13.

<sup>17</sup> Point also made by Cohen in Cohen 2000, p. 1437;

<sup>18</sup> L. LESSIG, *supra* note 13.

<sup>19</sup> Point also made in G. CALABRESI, A. D. MELAMED, "Property rules, liability rules, and inalienability: one view of the cathedral", *Harvard Law Review*, 1972, No 85.

away except when sold by the holder voluntarily at the price set by the holder.<sup>20</sup> Whereas the property rule protects the entitlement, the liability rule allows and ensures that the transfer thereof is possible provided the holder of the entitlement is compensated for his loss against “an external, objective [i.e. set by a third party] standard of value.”<sup>21</sup> Based on this understanding, because no other way to transfer the entitlement (in data) but via voluntary transaction with data subjects is allowed, Lessig’s model works in theory and property in personal data motivates the information industries to enter negotiations with data subjects and, as a result, implement PETs.

The validity of Lessig’s theory has been questioned on numerous grounds already in the US context. Among others, Litman doubts whether the understanding of property employed by the theory at hand corresponds to the actual law,<sup>22</sup> and how effective the whole enterprise to promote investments in PETs can be.<sup>23</sup> An extensive analysis of the validity of the theory in question under the US system goes beyond the scope of this paper. The following section attempts to ‘test’ Lessig’s theory in the European context.

### III. VIABILITY OF THE INSTRUMENTALIST THEORY IN EUROPE

The analysis of the viability of Lessig’s propertisation argument in the European settings may be broken into two parts: one may consider Lessig’s proposal on its face and on substance. The former approach leaves aside the content of the proposed property rights and merely focuses on propertisation of personal data in Europe as a formal possibility. The question to be answered here is whether introduction of the property rights in personal data, whatever scope of those rights may be, is a legal option in the European Union (you focus on the EU: make clear more earlier in your paper). A mere lack of competence to create these new rights is sufficient to discredit Lessig’s theory - as applied to Europe - on formal grounds. The latter - substantive - approach looks deeper into the

---

<sup>20</sup> *Ibid.*, p. 1105.

<sup>21</sup> *Ibid.* p. 1106, text in the square brackets added.

<sup>22</sup> Based on the definition of property given in the Restatement, Litman argues that “the *raison d’être* of property is alienability; the purpose of property laws is [not to prevent but to encourage and] ... prescribe the conditions for transfer.” Restatement of Property, §489 cmt. a (1944) referred to in J. LITMAN, “Information Privacy/Information Property”, *Stanford Law Review*, 2000, No 52, p. 1283, at p. 1295, text in the square brackets added.

<sup>23</sup> Litman labels Lessig’s argument “a fairy-tale picture”: industries do not respect information privacy because it is expensive to honour privacy preferences, not to express them. (*Ibid.*, p. 1297).

argument and considers the actual content of the proposed rights in order to establish whether they are consistent with the European notion of property. The following analysis will proceed along these lines and consider the viability of Lessig's instrumentalist theory when applied to Europe "on its face" and "substance".

I. *Lessig's instrumentalist theory on its face: is propertisation of personal data a legal option in Europe?*

To establish if propertisation of personal data may be a legal option in the system of the European Union, one may think of two possible ways in which propertisation may happen. The decision to substitute the current system of data protection via regulation by property rights may be taken either on the level of the European Union or by the individual Member States. The question to be answered at this stage is the one of competence, *i.e.* if the EU and individual Member States have the legal power to make such a decision.

When examining the EU competence, let's rest our analysis on the assumption that regulation in the area of data protection lies within the scope of the EU powers. Without going into details of the basis of such regulation in the European Treaties, the existence of the 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<sup>24</sup> is a good evidence of such a competence. However, the case of *propertisation* of personal data requires additional consideration since it involves not only the area of data protection, but also the subject-matter area of property rights. Whether the EU has a competence to force Member States into propertisation of personal information and to regulate (this sector of) property law is the question that needs to be answered.

The first step on the way to the answer is to acknowledge that introduction of property rights in personal data on the EU level would effectively mean harmonisation of a (newly created) sector of property law. Propertisation of personal data would not be the first area where the issue of the common European law of property is discussed. According to Van Erp, "several Directorates General are working on various projects concerning harmonization of property law."<sup>25</sup> A debate has been going on whether the structure of the Common Framework of Reference (CFR), a project meant "to restructure existing European private law and to be a

---

<sup>24</sup> Hereinafter referred to as EU Data Protection Directive.

<sup>25</sup> S. VAN ERP, "European and National Property Law: Osmosis or Growing Antagonism?", *Walter van Gerven Lectures*, Europe Law Publishing, 2006, p. 9;

“toolbox” for future European private law<sup>26</sup> should cover assignment of claims, personal security rights, security rights in movables, related matters in property law. Although Art. 295 of the European Community Treaty<sup>27</sup> seems to ban the EU intervention in property law issues,<sup>28</sup> in practice the effect of this Article is more restricted than one would assume at first sight<sup>29</sup> and has been interpreted more likely “to address the member states’ competence in nationalization and privatization.”<sup>30</sup> Moreover, some EU legislation in the area of property law has already been passed.<sup>31</sup>

Given that information industry and *de facto* market in personal data have already become a large part of the European economy and personal data long have been treated as a good, a possible legal ground for creating property rights in personal information on the EU level could be Art. 95 EC. To have Art. 95 EC as legal basis, the measure has to be necessary to attain the establishment and functioning of the internal market.<sup>32</sup> To qualify as such, according to Art. 14 EC, the measure should be aimed at establishing an area where free movement of goods, persons, services and capital is ensured. A top-down introduction of uniform property rights in personal data would certainly address the issue of free movement of the data within the EU without obstacles of different legal regimes.

The question to be answered next is whether the aim of ensuring free movement of personal data can be legally achieved by a measure of such level of detail as the one of establishing property rights. As the subsequent analysis will show, the provisions on powers of the EU may be interpreted in a way allowing even such an extensive intervention as top-down propertisation. That can be decided based on the subsidiarity principle as laid down in Art. 5 EC, Art. 2 TEU and Protocol 30 to the EC Treaty on the application of the principles of subsidiarity and proportionality. Art. 5 EC reads that the Community shall take action in areas which do not fall within its exclusive competence, in accordance with the principle of

<sup>26</sup> *Ibid.*, pp. 10–11.

<sup>27</sup> Hereinafter referred to as EC Treaty.

<sup>28</sup> Art. 295 EC: “This Treaty shall in no way prejudice the rules in Member States governing the system of property ownership.” For possible reasons of such treatment of property law see, e.g. D. CARUSO, “Private Law and Public takes in European Integration: the Case of Property”, *European Law Journal*, 2004, No 10(6), pp. 751–765. (“For the Union to signal that property rules will not be easily tinkered with is a highly symbolic gesture in the spirit of subsidiarity.”)

<sup>29</sup> S. VAN ERP, *o.c.*

<sup>30</sup> M. J. MILO, (2006). “Property and Real Rights.” *Elgar Encyclopedia of Comparative Law*. J. M. Smith, Edward Elgar: 587–602, p. 588;

<sup>31</sup> For more detail, see: *Ibid.* and S. VAN ERP, *o.c.*

<sup>32</sup> E.C.J., Case C-376/98, *Federal Republic of Germany v. European Parliament and Council of the European Union*, 5 October 2000 (so-called ‘Tobacco case’).

subsidiarity, only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States and can therefore, by reason of the scale or effect of the proposed action, be better achieved by the Community. The idea behind is that matters should be dealt with on the level closest to the ones affected.<sup>33</sup> However, as many commentators of the EU law point out, the very reason of existence of the European Union will “often demand Community action to ensure the uniformity of *general approach* which is of central importance to the realization of a common market.”<sup>34</sup> The subsidiarity principle, however, may have an effect on the form of the Community action for propertisation which may be through framework directives or guidelines rather than regulations.

The remaining question of competence is whether the individual Member States may take an action independent on the EU and introduce property rights in personal data. Such an action would not be a complete novelty since, as Milo rightly points out, property law has traditionally been “national law par excellence,”<sup>35</sup> since the national rules of private international law mainly rely on the principle of *lex rei sitae*,<sup>36</sup> i.e. the law applicable to an object in an international property law case is derived from the jurisdiction where the object is situated.”<sup>37</sup> However, in light of the fact that the EU has already taken action in the field of data protection in the form of the EU Data Protection Directive, the Member States will not be able to unilaterally introduce property rights in personal data the scope of which would substantially differ from the general approach to treating personal data adopted in the Directive. Any propertisation on the level of the individual Member States will have to be in line with the Directive. Even more, the Directive has been adopted with a view to leave a margin for the Member States to adopt actions which would respect the national legal systems, yet achieve the goals established in the Directive. Provided property rights introduced do not contradict those guidelines, a Member State which decided in favour of propertisation may serve as a laboratory to test the workability of the idea.

The above analysis shows that the idea to introduce property rights in personal data may be a legal option in the EU, both on the level of the Union and individual member states, although only the former may

---

<sup>33</sup> P. CRAIG, G. DE BÚRCA, *EU Law: Text, Cases and Materials*, Oxford University Press, 4<sup>th</sup> ed., 2008, p. 104

<sup>34</sup> *Ibid.*; see also A. ESTELLA, *The EU Principle of Subsidiarity and its Critique*, Oxford University Press, 2002, pp. 113-114.

<sup>35</sup> M. J. MILO, *o.c.*, p. 587.

<sup>36</sup> Emphasis added..

<sup>37</sup> M. J. MILO, *o.c.*, p. 587.

introduce propertisation altering the current general approach to data protection. The conclusion that follows is that Lessig's proposal understood on its face withstood the test. The focus of the next section is on whether it withstands the examination on its substance.

2. *Lessig's instrumentalist theory on its substance: propertisation as an engine of the general system of data protection?*

The purpose of the following analysis is to demonstrate that although Lessig's theory withstands scrutiny on its face, it is not viable when it comes to the actual substance of the argument. To examine the value of Lessig's theory for Europe on its substance, one has to consider the actual content of the rights labelled by the theory at hand "property rights." As it has been explained earlier in this paper, Lessig's argument operates with the definition of property given by Calabresi and Melamed<sup>38</sup> by opposing it to the liability rule. When the entitlement is protected by a property rule, it cannot be taken away except when sold by the holder voluntarily at the price set by the holder.<sup>39</sup> Therefore, property rule protects the entitlement, whereas the liability rule allows and ensures that the transfer thereof is possible provided the holder of the entitlement is compensated for his loss against "an external, objective standard of value."<sup>40</sup> Because no other way to transfer the entitlement (in data) but via voluntary transaction with data subjects is allowed, property rule motivates industries to respect privacy choices of the individuals and invest in PETS thereby bringing the general data protection system into action. Thus, there are two elements of the proposed property rights essential to Lessig's argument: in their core Lessig's property rights are there to protect entitlement rather than transfer, but simultaneously, leave a right holder an option to waive the entitlement for established price in the process of voluntarily transaction. The subsequent two parts of the paper will examine each element against the background of the EU legal system. In general, in this section the point will be made that in the context of the European legal system, first, the right to waive entitlement to data protection although not prohibited, is not protected against state intervention. Second, the proposed scope of rights does not fit into the European understanding of property, namely, that traditionally property law has been securing commerce, *i.e.* transfer, rather than preservation of the entitlement.

1. *Lessig's approach versus the doctrine of waiver of fundamental rights*

The first European-centered criticism of Lessig's approach rests on the assumption that, legally speaking, data protection is an element of the

<sup>38</sup> G. CALABRESI, A. D. MELAMED, *o.c.*

<sup>39</sup> *Ibid.*, p. 1105.

<sup>40</sup> *Ibid.* p. 1106, text in the square brackets added.

fundamental right to privacy as secured by Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms<sup>41</sup> and therefore enjoys full protection of a fundamental right.<sup>42</sup> As a part of such protection, it is an established position of jurisprudence (*Mellacher* case)<sup>43</sup> and the literature that the ECHR does not protect a right to obtain remuneration for the waiver or sacrifice of a fundamental right, as in an individual cannot claim a violation when the state prevents him, e.g. via regulation, from waiving a fundamental right.<sup>44</sup>

An alternative view is represented by, e.g. Paul De Hert and Serge Gutwirth.<sup>45</sup> They consider the categories of privacy and data protection against a background of a democratic constitutional state and as a result define them as two too distinct tools of state power control to be considered as one fundamental right.<sup>46</sup> Cuijpers argues that data protection is not a fundamental right. Therefore, freedom of contract has precedence over the rules of the 1995 EU Directive on processing of personal data, and the right to data protection may be waived or contracted around.<sup>47</sup>

There has been no authoritative pronouncement by the European Court of Human Rights or any other authority directly deciding in favour or against classifying data protection (both in public *and* private sector) as a fundamental right. The jurisprudence of the European Court of Human Rights is clear on including data protection into the scope of Art. 8 ECHR protection of private life when public authorities are involved. The Court's interpretation of Art. 8 ECHR right to respect of private life is said to correspond "with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose

---

<sup>41</sup> Hereinafter referred to as ECHR.

<sup>42</sup> The relationship between privacy and data protection is too complicated an issue to be fully discussed within the limited scope of this paper.

<sup>43</sup> E.C.H.R., *Mellacher v. Austria* (1989) 12 E.H.R.R. 391.

<sup>44</sup> O. DE SCHUTTER, "Waiver of Rights and State Paternalism under the European Convention on Human Rights", *Northern Ireland Legal Quarterly*, 2000, No 51, p. 487, at p. 506.

<sup>45</sup> P. DE HERT, S. GUTWIRTH, "Making sense of privacy and data protection: a prospective overview in the light of the future of identity, location-based services and virtual residence in the Institute for Prospective technological studies", in: *Security and Privacy for the citizen in the post-September 11 digital age: a Prospective overview*, European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), 2003.

<sup>46</sup> DE HERT and GUTWIRTH, p. 134.

<sup>47</sup> C. M. K. C. CUIJPERS, "A private law approach to privacy; mandatory law obliged?" *SCRIPT-ed*, 2007, No 4(4), pp. 304-318.

purpose is “to secure ... for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy with regard to automatic processing of personal data relating to him” (Article 1), such personal data being defined in Article 2 as “any information relating to an identified or identifiable individual”.<sup>48</sup> ... Art. 8 is applicable “where it [personal information – N.P.] is systematically collected and stored in files held by the *authorities*”<sup>49</sup> [emphasis added]. However, there is no similar ruling concerning ill data processing practices in private sector.<sup>50</sup> This partially can be explained by the nature of the European Convention as an international treaty creating obligations for its signatories, i.e. states. To rule finally on the applicability of Art. 8 to the private sector data processing, two issues of a more ground nature have to be decided first: whether Art. 8 of the Convention creates positive obligations for the contracting parties, and if it has horizontal effect.<sup>51</sup> Although of a principal importance, this discussion is too big and does not fit into the limited scope of this contribution. However, if, as the author believes, the fundamental right to privacy comprises data protection *also* in dealings of private parties, transactions in which individuals waive their entitlement in personal data in return for remuneration or services are not enforceable on the level on the ECHR and therefore not guaranteed against ban by the individual Member States. Although that does not exclude the possibility of waiver, it has to be taken into account.

Another important remark that can be made at this point is that unenforceability of waiver is only a policy choice enshrined in the current jurisprudence of the European Court of Human Rights in Strasbourg. As any policy decision, it can be changed following numerous proposals to drop the idea of paternalistic state and let people trade their rights and thus take more charge. However, this change has not been made yet, unenforceability of waiver is the law of the day and has to be taken into account.

### 3. *Lessig's approach versus European property law principles*

The last, and probably most decisive piece of criticism of the value of Lessig's theory for Europe which this paper advances is that property

<sup>48</sup> See: E.C.H.R., *Amann v. Switzerland* [GC], 16 Feb. 2000, App.No.27798/95.

<sup>49</sup> E.C.H.R., *Rotaru v. Romania*, 4 May 2000, App. No. 28341/95.

<sup>50</sup> Although there is a series of E.C.H.R. cases dealing with data protection on business premises, intervening actors are still public authorities (e.g. E.C.H.R., *Copland v. UK*, 7 Apr. 2007, app. no. 62617/00: public school authorities monitoring applicant's e-mail and phone calls).

<sup>51</sup> For a more detailed discussion on the horizontal effect of the ECHR see, e.g. D. GOMIEN, D. HARRIS, L. ZWAAK, *Law and Practice of the European Convention on Human Rights*, Strasbourg, Council of Europe Publishing, 1996.

rights defended by Lessig do not fit into the European framework of property law. The following analysis will demonstrate how.

To say that a certain understanding of property does not fit into the European idea thereof is a rather bold statement. Indeed, it would imply existence of a uniform approach to the concept of property throughout Europe. However, there is no such uniform approach to property. Each Member State determines the scope and regime of property rights independently. Besides purely national differences in defining and treating property, there is another major obstacle on the way to uniformity, *i.e.* common law-civil law divide. This allows different theories of property rights flourish simultaneously and take place in the property discourse which otherwise would be occupied by a statutory or case-law definition.

To reflect on the multiplicity of different types of property (also varying from one national legal system to another), Harris in his book *Property and Justice* develops a spectrum of the ownership interests ranging from a 'mere property' to 'full-blooded ownership'<sup>52</sup>. In case of a mere property, "the idea of property comprises the notion that something that pertains to a person is, maybe within drastic limits, his to use as he pleases and therefore his to permit others to use gratuitously or for exchanged favours. ... It embraces some open-ended set of use-privileges and some open-ended set of powers of control over uses made by others."<sup>53</sup> That has been also referred to as *erga omnes* effect or trespassory rule. An example of such a mere property right according to Harris' classification may be a right of a tenant with regard to the leased apartment. Although he cannot alienate the object of the right, he still may exclude even his landlord, the 'owner,' from entering the flat. This understanding is more characteristic of common law systems. At the upper end of the ownership stands so-called 'full-blooded ownership,' a relationship between a person and a resource when the person is free to do what he pleases with his own, "whether by way of use, abuse, or transfer"<sup>54</sup> To describe this type of the ownership interest, scholars refer to Blackstone and his Commentaries where he expresses the idea of the full alienability.

Despite such a wide range of different understandings of property rights, as it has been shown earlier in this paper, efforts to overcome differences and develop a pan-European property law (although only in some sectors) have already been taken. Behind those efforts lies impressive work of comparative legal scholars who, after analysis of the property laws in the

---

<sup>52</sup> J. W. HARRIS, *Property and Justice*. Oxford, Clarendon Press, 1996, p. 27.

<sup>53</sup> *Ibid.*, p.28.

<sup>54</sup> *Ibid.*, p.29.

European national legal systems have arrived at the conclusion that “it will certainly be possible to find common thought patterns”<sup>55</sup>. The analysis of this paper rests in particular on the work of professor Van Erp and his lecture *European and National Property Law: Osmosis or Growing Antagonism?*<sup>56</sup> He explains that such drastic differences between property rules of national legal systems are often a result of historical developments, the needs of legal practice, case law and academic legal analysis.<sup>57</sup> However, Van Erp continues, the differences are lying on the surface, on the level of technical rules, whereas more core norms and rationales – leading principles and ground rules – are shared and those are those core norms and rationales that have to be considered.<sup>58</sup> To evaluate how Lessig’s property rights fit into the European legal context, let us examine them against those leading principles and ground rules.

In Van Erp’s classification, leading principles of property law are “the filters through which a legal relationship must pass, before it can be characterized as a property right”<sup>59</sup> and not a personal (e.g. contractual) right. The leading principles are *numerus clausus* (content and number of property rights is limited, since property rights are the rights against the world with *erga omnes* effect) and *transparency* (given that they are against the world, others must be able to know about those property rights, when possession of an object is not decisive – by means of registration).<sup>60</sup> Transparency principle promises to be difficult but possible to respect in case of propertisation of personal data. Since the possession of data is not obvious, some kind of registry of property rights in personal data similar to the ones applied in the area of intellectual property may be created. Lessig’s property rules also seem to meet the *numerus clausus* and *erga omnes* classifications, since the entitlement protected by those property rules is against the world. However, so do the liability rules – the opposite of property rules in Melamed and Calabresi’s (and Lessig’s) classification.

However, the main obstacle for implementing Lessig’s theory in Europe on its substance lies in the ground rules of property. According to Van Erp, they describe the consequences of the establishment of a property right and “focus on how property rights relate among themselves.”<sup>61</sup> These rules

---

<sup>55</sup> S. VAN ERP, “European and National Property Law: Osmosis or Growing Antagonism?”, 2006, p. 13.

<sup>56</sup> *Ibid.*

<sup>57</sup> *Ibid.*

<sup>58</sup> *Ibid.*

<sup>59</sup> *Ibid.*

<sup>60</sup> *Ibid.* pp. 14-15.

<sup>61</sup> *Ibid.* p. 16.

are: the *nemo dat* (or *nemo plus*) rule, according to which one cannot give away more than one has; the *prior tempore rule*, according to which the oldest property right has priority over a younger property right over one object; limited rights have priority over fuller rights, and protection rules such as the right to (re)claim the object of the property right.<sup>62</sup> However, behind these principles and rules lie certain policy choices, in particular, the protection of commerce above protection of the original owner.<sup>63</sup> For instance, although according to *nemo dat* rule, one cannot give away rights which he did not have, it is counterbalanced by rules on third party protection. As Van Erp explains, a third party who acquired a right and paid for it in good faith, is often protected against the original owner, who claims his right of ownership.<sup>64</sup> Protection of a transfer seems to have priority over the entitlement in the European system of property law. Such rationale is not compatible with the principle division drawn by Melamed and Calabresi between property rules and liability rules based on the fact that the latter protected the transfer, whereas the former protected the entitlement.

The above analysis makes it legitimate to conclude that content-wise Lessig's instrumentalist theory does not fit into the European legal context because the scope of rights in personal data it advocates for is not what is meant by property in Europe. In case property rights in personal data are introduced in Europe, they will not be able to play the role of that engine which brings into action Lessig's general system of data protection comprising law, market, and technology. Ironically, what does approximate the function of such an engine is already existing system of data protection via regulation. If we recall the two core elements of Lessig's property rights, they are there to protect entitlement rather than transfer, and simultaneously, leave a right holder an option to waive the entitlement. The question of waiver being considered earlier, this is the general system of protection of human rights and of data protection in particular that secures the entitlement and prevents illegitimate transfer.<sup>65</sup>

#### IV. CONCLUSIONS

The ambition behind this paper was to test the viability of Lessig's instrumentalist theory of propertisation in the context of the European

---

<sup>62</sup> *Ibid.* pp. 16-17.

<sup>63</sup> *Ibid.* p. 17; see also on the principle of predictability and protection of commerce M. J. MILO, *o.c.*, p. 587.

<sup>64</sup> S. VAN ERP, "European and National Property Law: Osmosis or Growing Antagonism?", 2006, p. 16.

<sup>65</sup> "Illegitimate" since prohibition of transfer of personal data in the information society is impossible.

legal system. For the purposes of the analysis, Lessig's propertisation argument was considered from two angles: on its face and on substance. The content of the proposed property rights left aside, it was established that propertisation of personal data in Europe is a formal legal possibility, both on the level of the European Union and individual Member States. Although, only the former may introduce propertisation altering the current general approach to data protection. The substantive analysis of Lessig's argument looked deeper into the actual content of the proposed rights. It was established that although propertisation of personal data in the EU is a legal option, it is suspect since it implies the possibility of waiver of the right to data protection, whereas such waiver is not enforceable in the system of ECHR against state intervention. The last, and probably most decisive piece of criticism of the value of Lessig's theory for Europe was that property rights defended by Lessig do not fit into the European framework of property law. Despite all differences between technical rules of the national property law systems, characteristic of the European approach to property is that protection of a transfer seems to have priority over the entitlement in the European system of property law. Such rationale is not compatible with the principle division drawn by Melamed and Calabresi between property rules and liability rules based on the fact that the latter protected the transfer, whereas the former protected the entitlement. Therefore, content-wise Lessig's instrumentalist theory does not fit into the European legal context because the scope of rights in personal data it advocates for is not what is meant by property in Europe. In case property rights in personal data are introduced in Europe, they will not be able to play the role necessary for Lessig's general system of data protection to function.

# THE MYTH OF ODIN'S EYE: PRIVACY VS. KNOWLEDGE

Paolo Guarda<sup>\*</sup>

## I. INTRODUCTION

Knowledge has always represented a sort of human unrealizable dream and omniscience, that means the complete and unlimited knowledge, is considered by most of the cultures as a divine characteristic. To know means to have the power: in human history – and in recent philosophical reflections – it is a full stop!

But what are we willing to give to get access to knowledge? Myths and stories on knowledge research tell of long trips and of supreme sacrifices. In the portrayals of Odin, the father of the gods in the Scandinavian tradition, he is often represented with a single eye<sup>1</sup>. One of the several changing Nordic legends tells that, in order to satisfy his thirst for knowledge, the god sacrificed his eye to Mimir, the Mimirsbrønd's keeper, the magic fountain of wisdom placed on Yggdrasil's roots<sup>2</sup>. Since then, the divine eye is situated in the icy water of the fountain, as the price paid to acquire the eyes of the sage and to discern the essence of things, behind the appearance.

This is the price paid by Odin. But what are we willing to pay? Or rather: are we really aware of the cost of our access to knowledge, particularly in the digital context and despite the outward gratuitousness of the provided service? I will try to give an answer to these questions in the following pages.

In the first part I will focus on the issues linked to utilization of Digital Rights Management systems (DRM), suited to regulate the fruition of intellectual works protected by intellectual property rules, with specific reference to users' privacy in its different dimensions; then, always from a privacy oriented point of view, I will outline the problematic aspects that open access to knowledge presents; I will analyze a paradigmatic example of free of charge service that poses monstrous risks from the point of view of users profiling activity. At the end, in order to pull the strings of the matter together and to take back the cues offered by Odin's saga, I will develop some final reflections on the relationship between privacy and

---

<sup>\*</sup> Ph.D. in Comparative Private Law, University of Trento

<sup>1</sup> For closer examination on Nordic saga, see V. GRØNBECH, *Miti e leggende del nord*, Torino, Einaudi, 1996 (Italian translation of the Danish edition *Nordiska Mita og Sagn*, Copenhagen, 1965).

<sup>2</sup> See *Völuspá* (*Prophecy of the Völva*), the first and the most famous of *Edda poems*.

knowledge in the digital context.

## II. INTELLECTUAL PROPERTY, DIGITAL RIGHTS MANAGEMENT (DRM) AND PRIVACY

The advent of digital technologies gave rise to two phenomena: on the one hand, we register a heightening of the rigid and concentrated control (i.e. the DRM systems), based on commercial rules; on the other hand, we have the coming of new ways to fruitions focused on open access rules.

I will concentrate on the hidden “price” that the user pays to get access to digital intellectual works, whether in the platforms that incorporate values and rules of the intellectual property, or in the architectures inspired by openness (I will analyse this issue in the next paragraph).

From a purely technological point of view, the information production model based on the information closure and the rigid and concentrated control of it is implemented through DRM systems<sup>3</sup>. This term singles out the most advanced anti-access and anti-copy protection system on the market. The heart of every DRM is constituted by two modules. On the one hand, the so called “content-module”, that contains the digitalized data (text or audio files) “secured” through a cryptography process and ready to be distributed; before it happens, the name of the author, the copyright owner, the creation date, the title, the format, the dimension, and other technical information in order to identify the file (i.e. the ISBN) are incorporated into the content. On the other hand, the “licensing-module” generates the digital license that guarantees to the final user the access to the contents in the light of the usage rights of business rules. These determine the “what”, that means the precise piece of content to be used, and the “when”, that means to link particular features to every right: the type of user authorized to assert the “right”, the extension of every right (duration or numbers of permitted utilizations), and the price in order to assert the right.

Let’s see an example so as to understand how this mechanism works<sup>4</sup>.

---

<sup>3</sup> In-depth analysis, see R. CASO, *Digital Rights Management. Il commercio delle informazioni digitali tra contratto e diritto d'autore*, Padova, Cedam, 2004 (digital reprint, Trento, 2006, available at the Web-site: <<http://eprints.biblio.unitn.it/archive/00001336/>>); A. PALMIERI, “DRM e disciplina europea della protezione dei dati personali”, in R. CASO (eds), *Digital rights management: problemi teorici e prospettive applicative. Proceedings of the Conference Trento Faculty of Law 21-22 March 2007*, Trento, Alcione, 2007, pp. 197 ff..

<sup>4</sup> The example, modified in the lights of the considerations I am developing, is partially taken from P. GANLEY, “Access to the Individual: Digital Rights

Suppose I wish to get access to the new publications of an on-line law journal. I registered myself giving my profile details to the portal that contains the journal: my data are saved in a database assigned to store information regarding the users' identity inside the licensing-module. At the same moment, the system generates the usage rules that sets the type of utilization, the cost, and the specific category of authorized users; then it puts all this information into the licensing-module. Whenever I desire to read the latest publication, the DocuReader device contacts the content-module and a decrypted copy is sent to my computer. Now I am able to display what I was looking for, but every future access attempts will be denied. In order to get other accesses, I will have to take out a subscription that will enable me to get more displays, or greater usage margins. This is a simple example of how a DRM system works.

The DRM system also presents functionalities that have a direct impact on user privacy<sup>5</sup>. It contains at least one of the following basic functions<sup>6</sup>:

- content access control;
- content usage control;
- content identification, content owners, and general condition of usage;
- authentication of identification data.

Moreover, for its own particular peculiarities, a DRM system is able to monitor the content fruition and, in case it has been set in that way, it can "sanction" the behaviours that are not compliant with its rules, for instance disconnecting the access.

Looking through what a DRM can do, a privacy scholar immediately thinks of "profiling"<sup>7</sup>. Personal data of Internet users, consumers of intellectual works, and, more generally, their commercial interests symbolise a real treasure for people working on the Net. The possibility of monitoring the user activities does not only represent the way to control-

---

Management Systems and the Intersection of Informational and Decisional Privacy Interests", *International Journal of Law and Information Technology*, 2002, p. 241.

<sup>5</sup> In the digital age law, privacy and copyright often know clashing points. See, for example, the case *Peppermint* annotated in R. CASO, "Il conflitto tra copyright e privacy nelle reti peer to peer: in margine al caso Peppermint. Profili di diritto comparator", *Dir. dell'Internet*, 2007, p. 471 (available at the Web-site: <<http://www.jus.unitn.it/users/caso/DRM/Libro/peppermint/home.asp>>).

<sup>6</sup> See R. CASO, *Digital Rights Management*, o.c., p. 100.

<sup>7</sup> On the profiling activity, see B. CUSTER, *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling Epidemiology*, Nijmegen, The Netherlands, 2004.

manage his digital content fruition in order to impose – and when it is supposed to be necessary to sanction – the behaviours allowed according to the license that regulates the usage rights; but it becomes also a way to commodify the profile itself: this profile can be used by the profiler to adopt a more effective marketing strategy (maybe through some advertising banners answering user interests) or becomes itself an exchanging good, when the information is sold to a third party.

This kind of considerations makes us easily understand the real impact that these technologies have with respect to users privacy. Now I need to clarify what I mean by the term “privacy”. When you deal with the description of this concept, even more if you place yourself by the point of view of the relation between law and technology, you tell how from a privacy intended as the “right to be let alone”, originating from the paper of great-renown of Warren and Brandeis<sup>8</sup>, we arrived to a meaning much more linked to the idea of control of personal data, thanks to digital technologies diffusion. And actually, when we say “privacy” referring to the provisions that regulate it, we immediately hasten to remember that we are talking of personal data, of data control, of information to data subject, etc.<sup>9</sup>.

But now I would like to quote a more extensive concept of privacy. This kind of description of the concept allows us to better understand the real importance of privacy in the Net, its actual role, in a context in which more and more information, and the commodification of it, comes into the limelight. People personality itself is taken to small pieces that are personal data. These pieces, once you have reassembled them, sketch out the profile of a person in the digital context, his virtual identity. The control on these pieces of identity has more dangerous repercussions than we can imagine if we take into account a narrow interpretation of privacy, since it involves the life fundamental aspects of the person to whom the data are related.

After all these expectations, I will describe which are these theories I was referring to. The consumption of intellectual works, intended as the fruition of work of the intellects and of other information, is directly linked to three fundamental dimensions of the concept of privacy:

---

<sup>8</sup> D. WARREN, L. D. BRANDEIS, “The Right to Privacy”, *Harvard L. Rev.*, 1890, vol. 4, p. 193.

<sup>9</sup> For closer examination on privacy regulation, see *ex plurimis* L. A. BYGRAVE, *Data Protection Law. Approaching Its Rationale, Logic and Limits*, The Hague – London – New York, 2002; P. GUARDA, “Data Protection, Information Privacy, and Security Measures: an Essay on the European and the Italian Legal Frameworks”, *Cyberspazio e dir.*, 2008, p. 65.

“spatial”, “informational”, and “decisional”<sup>10</sup>.

The first dimension, the “spatial” one, concerns the physical space, and in particular the size of the area in which the solitude of a person is protected from external invasion: this kind of privacy corresponds to a particular idea that sociologists connect to the relation between the private and the public space. The dimension I am talking about is related to freedom from external nuances or, more generally, from every kind of source of disturbances coming from the outside. In the matter I am dealing with now, spatial privacy involves those spaces in which a person is at liberty to behave in such a way that would be considered aberrant by the point of view of the dominant social norms or, more plainly, not normally used in public.

The second dimension, “informational” privacy, regards the flow of personal information. More accurately, it relates to the individual control with respect to processing of his personal data. Therefore, it is directly linked to that conceptualization of privacy focused on the control and the regulation of personal data treatment. From the point of view that focuses on the impact of DRM systems, processed data are information regarding the intellectual consumption, acquired by means of the functionalities we saw typifying the technological protection measures.

The third, and certainly most important, dimension of privacy is the “decisional” one: it concerns the choice, the freedom that must be recognized to every person in order to be able to take a decision without any kind of external conditioning. I wish to focus my attention on this dimension.

The “decisional” privacy involves the essence itself of human being. The free will, the freedom of self-determination, ultimately the freedom to be a man. There is not law, if there is not free will, if there is not the possibility to choose, even if to be wrong. Therefore, the violation of this dimension straightforwardly affects the “capacity” to be a man. The monitoring activity, the awareness of being spied on, the consciousness that the

---

<sup>10</sup> See J. KANG, “Information Privacy in Cyberspace Transactions”, *Stan. L. Rev.*, 1998, vol. 50, p. 1193, at 1202-1205; P. GANLEY, “Access to the Individual”, *o.c.*, at 251 ff.. Professor Caso draws from an American commentator a double dimensions of the concept of privacy (informational and spatial): R. CASO, *Digital Rights Management*, *o.c.*, p. 103 ff.; J. COHEN, “DRM and Privacy”, *Berkeley Tech. L.J.*, 2003, vol. 18, p. 575. More generally, on the implications of DRM systems with respect to privacy and freedom of speech, see I. KERR, J. BAILEY, “The Implications of Digital Rights Management for Privacy and Freedom of Expression”, *Info., Comm. & Ethics in Society*, 2004, vol. 2, p. 87.

context around us is unceasingly changing in the light of the profile that other people are designing to us, modify person's behaviour. The famous Panopticon of Bentham was based on this idea<sup>11</sup>: the radiocentric form of the building and the appropriate architectural and technological contrivances, that enabled a single warden to watch all the prisoners at every moment, without the possibility for these to establish if they were actually controlled or not (this point reminds us dreadfully the monitoring on the Net), gave the inmates the sentiment of an invisible omniscience, influencing their behaviour and persuading them to not violate the rules.

Therefore, the perception of being watched influences, and will influence, our intellectual consumption, in such a way that we probably are not yet able to clearly determine.

Let's go back to the example I was using to better understand the potential consequences of DRM systems with respect to privacy.

Before the published content in the on-line law journal has been encrypted, a metadata, called "Digital Object Identifier" (DOI), is inserted into every section of all the articles. The granularity level of this DOI (every article, every section, or every paragraph), that are unique for every type of content, is decided by the editor. The outcome of this process is the following: all crypted data in the content-module are directly linked to some "pieces" of identifier metadata, that will always remain in the content when this is subsequently distributed. Then, every time I wish to modify the content of the document I have asked to the system (for instance to open, display, print a specific section of the publication), the "ContentControl" application sends an information package to the licensing-module, inclusive of the DOI and of the details of the action carried on; the package will be stored in the "logging program". Simply accessing to the licensing-module, the editor can compile aggregate statistics of the utilization of the contents or display the profile of a specific user combining the information stored in the logging program with data saved in the database suited to collate users personal information.

### **III. "FREE OF CHARGE" ON-LINE INFORMATION ACCESS SERVICES AND PRIVACY**

I will deal in this section with the other moon's face: the Open Access

---

<sup>11</sup> J. BENTHAM, *The Panopticon Writings*, edited by M. BOZOVIC, London, Verso, 1995. Bentham himself described the Panopticon as "a new mode of obtaining power of mind over mind, in a quantity hitherto without example".

world or, more in general, the open – and seemingly free of charge – access to the fruition of on-line information<sup>12</sup>. I will hold the “Google” search engine as a paradigmatic example, also in its versions of “Google Scholar” and “Google Book Search”<sup>13</sup>. I made this choice since it represents a model, among the most invasive ones in the Net, of personal data gathering and of users profiling. Obviously, many of the issues I am going to describe can be met in other portals that provide access to scientific knowledge, especially when they are provided by an authentication system.

From a purely economic point of view, this scenario could seem as an ideal world, that is the world of the free of charge and completely open access to knowledge; unfortunately, it is actually hiding a dark side. Notwithstanding the outward idyll, also in this context we are paying, often completely unawares, a very expensive price.

Google is one of the most evident examples of personal data collection and, more generally, of information related to users. Every day millions of people use this search engine, giving to it information regarding their interests, needs, desires, fears, etc..

I want to begin with a starting remark: Google is recording every query and is connecting them to a given Internet Protocol address (IP). This sentence probably frightens, astounds, immediately makes us calling to mind all the queries we have done, fearful of “what did we ask to Google?”.

Let's proceed in order. From this point of view, privacy concerns personal data, the information that European Directive 95/46/EC (“on the protection of individuals with regard to the processing of personal data and on the free movement of such data”) at article 2, lett. a, defines as relating to “an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”. Hence, in reverse order, information that cannot be connected with a specific person is not a privacy issue. Then, the question lies in the possibility to establish this connection.

---

<sup>12</sup> For a closer examination on Open Access issues, see R. CASO, *Ricerca scientifica pubblica, trasferimento tecnologico e proprietà intellettuale*, Bologna, Il Mulino, 2005, p. 312; ID., “Proprietà intellettuale, tecnologie digitali ed accesso alla conoscenza scientifica: Digital Rights Management vs. Open Access”, available at the Web-site: <<http://eprints.biblio.unitn.it/archive/00001407/>>.

<sup>13</sup> I took as a point of reference of this part: O. TENE, “What Google Knows: Privacy and Internet Search Engines”, (October 2007), available on the Web-site: <<http://ssrn.com>>.

In the following part I will explain how the log files relating to our queries can be associated to our person (*rectius*, identity).

First of all, it happens through the IP collection. These are numbers that identify unequivocally the devices connected to a single network; IPs can be statics, that means fixed, or dynamics, that means assigned each time by the Internet Service Provider (ISP) to his subscribers depending on necessity. The IP address, that can be banally considered the equivalent of a street address or of a telephone number, is regarded a personal data according to art. 2 Directive 95/46/EC (and art. 4, Italian Data Protection Code)<sup>14</sup>. Even if Google is not able to match the IP address linked to the log file that contains the queries, to a certain user, the fact that the ISP has this kind of data and that the public authority could force him to communicate data relating to the subscribers makes the log files close to personal data.

In the second place, to overtake the difficulty of profiling users caused by dynamic IP addresses, an open access service portal can use “cookies”: these mark the user browser (the application used for surfing in the Net) with some “unique identifying numbers”<sup>15</sup>. Actually these files, that are supposed to facilitate users in remembering their login data and queries at every connection to the same Web page, permit the search engine to recognize the user as a “recurrent visitor” of the site and to collate the history list of his queries, even if he connects to the Net using different IPs<sup>16</sup>.

Cookies in themselves cannot be considered personal data, since they identify a particular browser (*rectius*, a computer), rather than a user. The cookie can be imagined as a sort of label, as “7583c03948le24”, without any visible repercussion on privacy, but as it were stick on a personal data box of an anonymous person. If you could match a given cookie, linked to a log file, with the queries on the search engine, to a specific person, then again

<sup>14</sup> See Opinion of Article 29 Data Protection Working Party 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, available at the Web site: <www.ec.europa.eu>.

<sup>15</sup> In-depth analysis, see J.J. THILL, “The Cookie Monster: From Sesame Street to Your Hard Drive”, *S.C. L. Rev.*, 2001, vol. 52, p. 921.

<sup>16</sup> Google has lately announced the intention to reduce the cookies retention period, initially stated until 2008, to “only” two years starting from the latest user search in its search engine: see “Cookies Expiring Sooner to Improve Privacy”, Official Google Blog, 16 July 2007, available at the Web site: <<http://googleblog.blogspot.com/2007/07/cookies-expiring-sooner-to-improve.html>>. If we think that we all use it almost every day, we immediately realize that this undertaking has very little impact on privacy.

you would relapse into the personal data uncomfortable – at least for the profilers – hat. But also this obstacle can be bypassed: let's see how. As everybody knows, in addition to the search engine, Google provides several additional services (from the e-mail account to the investment portfolio) that are subject to registration through credentials, as the real name or the e-mail address (the most obvious example is Gmail). At this point, Bob's your uncle: the user logs into the Internet, loads the search engine portal, in the meanwhile he introduces a query. Google uses the same cookie to identify the list of queries and the e-mail account: the cookie anonymity is once and for all lost, the missing name on the users' interests log files box has now a name and a surname!

In the end, a final possibility to collate personal data is left over: this time the only guilty party is the user himself, apart from every kind of tactics he could adopt to reduce the use and the identification of his cookies. We all have tried in our life to look for our name on Google or, in our specific case, to search for our essays on a scientific database, maybe repeatedly in the same year<sup>17</sup>. These queries are called “ego searches” or “vanity searches”. They allow the profiler to link the information relating to users interests to a certain identity.

Now let's put another question to ourselves: where do the log files containing all these information on our queries go to?

In the Google privacy policy we find innocently stated: “We use cookies to improve the quality of our service by storing user preferences and tracking user trends, such as how people search. Most browsers are initially set up to accept cookies, but you can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some Google features and services may not function properly if your cookies are disabled”<sup>18</sup>. Thus, the declaimed reason lies in the wish to improve the quality of the service! What's a pity if we understand that in the meanwhile Google is starting the most extended and unprecedented in human history “Database of Intentions”: “the aggregate results of every search ever entered, every result list ever tendered, and every path taken as a result”<sup>19</sup>. Incentives to maintain this huge amount of information are represented

---

<sup>17</sup> See C. SOGHOIAN, “The Problem of Anonymous Vanity Searches”, Winter 2007, available on the Web-site: <<http://ssrn.com>>.

<sup>18</sup> See “Google Privacy Policy”, available on the Web-site: <<http://www.google.com/intl/en/privacypolicy.html>>.

<sup>19</sup> Term taken by J. BATTELLE, “The Database of Intentions”, *John Battelle's Searchblog*, 13 November 2003, available at the Web site: <<http://batelmedia.com>>; see also ID., *The Search: How Google and its Rivals Rewrote the Rules of Business and Transformed our Culture*, Boston, MA - London, Nicholas Brearley Publishing, 2005.

by: the relatively low gathering and maintaining costs, the lack of a unique and clear regulation on this issues (this even more in the US legal system), and the very remunerative potential utilization of information.

The Database of Intentions symbolizes also a very valuable good, a sort of goldmine if we take into account the economic value of information contained, that are a great temptation for many people: national security agencies, hackers, identity thieves, etc.. Just now, the search engine provider are not allowed (or should not be allowed) to sell personal data to third person. Hereafter it does not mean that it is not going to be allowed in the future, they exchange user data with subsidiary companies or other trusted business partners, in order to process this information and to provide services<sup>20</sup>.

However that may be, there is always a third part with respect to data processing that could try to obtain personal data communication from the search engines, through a completely lawful procedure. I am referring to public authorities that could be interested in using log files for national security purposes. Especially after the tragic event of September 11<sup>th</sup>, an in progress trend is modifying the way in which citizens consider the State and its tasks, and is gaining force, remarking the traditional role of public security guardian. At the beginning the State was remaining in the background in Internet regulation, but now it is more and more starting again to play a protagonist role, making strategic alliances with ISPs: these person are in possession of very precious information for prevention and contrasting activities against criminality. Then, we talk about "Invisible Handshake"<sup>21</sup>.

I took into account the Google example, but the same considerations could be developed for the scientific specialized portals that offer services of the same kind. Actually most of them require a prior necessary authentication in exchange for the download of full text materials proposed by the Web site (otherwise you are allowed to get only the abstract of the paper: see, as example, the Social Science Research Network (<http://ssrn.com>)).

---

<sup>20</sup> Again in the Google Privacy Police we read: "We offer some of our services in connection with other web sites. Personal information that you provide to those sites may be sent to Google in order to deliver the service. We process such information in accordance with this Policy. The affiliated sites may have different privacy practices and we encourage you to read their privacy policies".

<sup>21</sup> See M.D. BIRNHACK, N. ELKIN-KOREN, "The Invisible Handshake: The Reemergence fo the State in the Digital Environment", *Va. J. L. Draft*, 2003, vol. 3., available at Web-site: <<http://ssrn.com>>.

#### **IV. CONCLUSION: TOWARD THE OVERCOMING OF PRIVACY VS. KNOWLEDGE CONFLICT**

At the end of the way I lead, let's pull together the strings of what I said, trying to unveil, if it is not already clear, what the Odin saga has to do with our issue.

Whether we are dealing with fruition of scientific knowledge under the proprietary schemes transposed in the digital context by DRM systems, or with free access to contents following the trend that brings to Open Access, we are losing (exchanging, if we were aware of that) our identity, our profile, our data in return for intellectual works we wish to enjoy. As it happened for Odin, we are handing over an eye, that means a very important part of our body, to Mimir, that is the holders of the knowledge we are so fervently seeking. Remaining on the same mythological example, other interesting – and at the same time appalling – similitudes occur to us. To drink by the magic fountain a gulp of knowledge we hand over an eye, and with that we are giving to other persons the possibility to see inside us through the given eye, to know what we think, what we desire, briefly speaking to appropriate our most hidden, and simultaneously most precious, part: our thoughts.

Privacy is not only characterized by the tridimensional concept I described before (spatial, informational, decisional). It represents also a cultural phenomenon: everybody must be fully aware of the risks connected to an unlawful data processing and becoming themselves the first “security measures”, proper to avoid illegal utilization of data. Until Internet users understand the risks connected to the processing of their personal data and the real cost they pay to get access to the several services offered by the Net, they will always be dreadfully exposed to the monitoring of all those who, on the contrary, commodified exactly this awareness.

Furthermore, we may had to say: scientific knowledge vs. privacy. And actually this conflict is manifest enough, I hope even more. But, if you really want to solve the contrast, you have to get over the traditional way to conceive the opposite poles.

Privacy does not consist only in making some rules, some restrictions, after all some obstacles to data circulation; it must be declined in the correct management of the flows of data that marks out the information age in an ineliminable way. Knowledge, on the other hand, knows the already famous phenomenon of dematerialization that changes books, poems, music, drawings, into files expressed in binary code. Maybe it does not anymore make sense to conceive both terms of our subject in a physical

way, carrying on a contrast that does not exist anymore in the digital context. It would be better to start reasoning on the fact that they can be considered as they are in the digital world, that is information, and thus reconsidering rules, technologies, and customs in the light of this new unifying category that moves our attention to the management aspect of the exchanging flows, rather than to their inherent diversity.

# GENETIC ENHANCEMENT AND AUTONOMY

Wojciech Załuski

## I. THE PROBLEM OF THE ADMISSIBILITY OF GENETIC ENHANCEMENT

The present paper deals with an oft-raised argument against the admissibility of enhancing an embryo's nature through genetic engineering (hereafter: genetic enhancement), namely, the argument from autonomy. The argument asserts that genetic enhancement is not admissible because it violates human autonomy (i.e., the autonomy of a person who is to grow up from the embryo subjected to genetic engineering). Clearly, in order to appraise this argument, one must have a clear understanding of the notion of autonomy. Accordingly, a large part of this paper is devoted to clarifying this notoriously unclear notion. The clarification proceeds in two stages. First, a distinction is made between personal and moral autonomy. Second, the concept of presuppositions of moral autonomy is introduced. It is argued that one can distinguish two conceptions of moral autonomy depending on whether one assumes that the contingency of birth is a presupposition of moral autonomy or not. In the final part of the paper, relations between the two conceptions of moral autonomy and two types of genetic enhancement ('directed' and 'all-purpose') are examined.

## II. AUTONOMY

### 1. *Two concepts of autonomy*

As it seems, there are two concepts of autonomy – personal and moral. As we shall see, personal autonomy has two varieties, and moral autonomy has three varieties.

#### a. Personal autonomy

Personal autonomy can be defined as the agent's freedom at the level of choosing her desires (preferences, goals). The somewhat vague phrase 'having freedom at the level of choosing one's desires' can be explicated in the following way: 'having the second-order capacity to distance oneself from one's first-order, i.e., action-guiding desires, to evaluate them in a critical way by considering reasons for their acceptance and for the acceptance of alternative desires, and to change them if they do not pass critical scrutiny'. The concept of personal autonomy has two varieties – material and formal. The formal variety does not forestall what desires (preferences, goals, etc.) an agent should choose (whether they be moral or amoral, whether they are to satisfy some ideal of human excellence or not,

whether they are to be loyalty, commitment, obedience to a group or rather some kind of substantive independence, whether they can be self-destructive or not). The only thing it requires is that an agent should be able to critically evaluate her first-order desires, and, should these desires not pass the critical evaluation, to change them. Accordingly, on this variant, a personally autonomous agent can be just as well a self-sufficient individualist insensitive to the needs of others as an altruist treating others' needs as one's own needs – just as well a villain as a saint, etc. By contrast, the material variety requires that an agent should choose a specific type of desires (moral, realising some ideal of human excellence, prudent, or rational, etc.).<sup>1</sup>

Three further remarks on the formal variety of the concept of personal autonomy are in order here. First, personal autonomy does not operate in an all-or-nothing fashion; rather, an agent may be personally autonomous to a higher or lesser degree. As it seems, though, no human being can be called an agent (i.e., the true author of her own actions) if she loses completely her personal autonomy. This is so because the agent's first-order, i.e. action-guiding desires can be really called *hers* only if she really wants to have these desires, i.e., if she has second-order desires to have and to realise her first-order desires. Accordingly, some level of personal autonomy is indispensable to human agency (though, as it must be admitted, it is difficult to determine what level exactly constitutes the threshold between agency and the lack of agency). As we shall see presently, the fact that in order to be called 'an agent' a subject must exhibit some level of personal autonomy is relevant to the question about the relations between personal autonomy and moral autonomy. Second, personal autonomy is a *value* – a desirable feature of human being. One can argue for this claim indirectly: personal autonomy is a value, as it is a necessary condition of human agency, or directly: personal autonomy is a value because the very capacity not to yield unreflectively to one's first-order desires is valuable in itself. Third, personal autonomy should be distinguished from freedom at the level of realising one's desires, i.e., from freedom understood as the lack of obstacles in realising one's desires. It is worth noting that an agent may be personally autonomous and free (in the sense 'encountering no obstacles in realising her desires'), personally autonomous and non-free, personally non-autonomous and free, and

---

<sup>1</sup>Defining autonomy as a second-order capacity, i.e., as a capacity to distance oneself from one's first order, i.e., action-guiding desires, is widespread in the relevant literature. Also my distinction between formal and material autonomy is not new. See, for instance, G. DWORKIN, *The Theory and Practice of Autonomy*, 6th ed., Cambridge, Cambridge University Press, 2001 (Dworkin writes about formal and substantive autonomy); H. G. FRANKFURT, "Freedom of the Will and a Concept of a Person", *Journal of Philosophy*, 1971, No 68, pp. 5-25.

personally non-autonomous and non-free.

Let me now turn to the second concept of autonomy – moral autonomy.

b. Moral autonomy

Moral autonomy can be defined as the agent's capacity to reflectively choose moral principles which are to govern her actions and/or reflectively affirm moral principles which she already accepts (and which she may have originally accepted on unreflective grounds), i.e., as the capacity for normative self-government. I shall call this understanding of moral autonomy 'the strong variety of moral autonomy' (to be distinguished from its two other varieties discussed below). This variety has a formal and material variant. The material variant specifies what moral principles an agent should reflectively choose and affirm if she is to be called 'morally autonomous', while the formal variant requires only that the agent should reflectively choose moral principles which are to govern her actions and/or reflectively affirm moral principles she already accepts.

Moral autonomy can be understood also in a weaker way – as the capacity to understand moral principles as a specific kind of reasons for action (i.e., as different from conventional rules) requiring obedience in an especially categorical way. I call this understanding of moral autonomy 'the weak variety of moral autonomy'. What this variety implies is that an agent understands moral principles *qua* moral principles. In other words, it implies that an agent can discern the specificity of moral principles which consists in that they (as opposed to conventional rules) constitute particularly strong reasons for action, i.e., reasons overriding other reasons for action. It does not imply that the agent has the capacity to reflectively choose moral principles and/or reflectively affirm principles which she already accepts. Of note is the fact that this variety of moral autonomy constitutes a cognitive element of the moral sense and thereby a condition of moral accountability (the second element of the moral sense is motivational – it is a tendency of the agent to comply with moral principles). Accordingly, an agent who commits a crime can be held morally accountable for her deed only if she exhibits a cognitive element of the moral sense (clearly, by definition, such an agent has a defective motivational element of the moral sense). Similarly to the strong variety of moral autonomy, one can also distinguish a material and formal variant of the weak variety of moral autonomy.

Apart from the strong and weak variety of moral autonomy, one should also mention about what can be called 'Kantian moral autonomy' or 'the strongest variety of moral autonomy'. Kantian moral autonomy can be

defined as the agent's capacity to reflectively choose moral principles which are to govern her actions and/or reflectively affirm moral principles which she already accepts, and – additionally – to be motivated by these moral principles alone, without interference of any empirical causes. Analogously to the weak and strong variety of moral autonomy, Kantian moral autonomy can also be divided into a formal and material variant. As can be readily seen, the formal variant of Kantian moral autonomy implies the formal variant of the strong variety of moral autonomy (which, in turn, implies the formal variant of the weak variety of moral autonomy).

The results of the analyses conducted in sections 1 and 2 can be schematically summarized in the following way:

*Personal autonomy*

- I. Formal variety (second-order capacity to choose one's first-order desires; it is not specified which desires should be chosen).
- II. Material variety (second-order capacity to choose one's first-order desires; it is specified which desires should be chosen).

*Moral autonomy*

- I. Weak variety
  - 1. Formal variant (understanding moral principles *qua* moral principles; moral principles are not specified).
  - 2. Material variant (understanding moral principles *qua* moral principles; moral principles are specified).
- II. Strong variety
  - 1. Formal variant (capacity to reflectively choose moral principles which are to govern one's actions and/or reflectively affirm moral principles which one already accepts; it is not specified which moral principles should be chosen).
  - 2. Material variant (capacity to reflectively choose moral principles which are to govern one's actions and/or reflectively affirm moral principles which one already accepts; it is specified which moral principles should be chosen).
- III. Strongest variety (Kantian moral autonomy)
  - 1. Formal variant (capacity to reflectively choose moral principles which are to govern one's actions and/or reflectively affirm moral principles which one already accepts, and to be motivated by these moral principles alone, without interference of any empirical causes; it is not specified which moral principles should be chosen).
  - 2. Material variant (capacity to reflectively choose moral

principles which are to govern one's actions and/or reflectively affirm moral principles which one already accepts, and to be motivated by these moral principles alone, without interference of any empirical causes; it is specified which moral principles should be chosen).

In the remainder of this paper, by personal autonomy I shall mean 'the formal variety of personal autonomy', and by moral autonomy I shall mean 'the formal variant of the strong variety of moral autonomy'. The narrowing down of my considerations to the two varieties of autonomy is due to the fact these two varieties seem to be the best explications of the concepts of personal and moral autonomy. The material variety of personal autonomy seems to be too strong: the requirement that an autonomous agent ought to choose a concrete type of first-order desires does not harmonize well with the notion of personal autonomy as it is usually used in the philosophical discourse. Besides, the material variety of personal autonomy becomes hard to distinguish from moral autonomy. As for moral autonomy, its weak variety seems to be too thin – moral autonomy seems to require something more than just the capacity to understand moral principles *qua* moral principles, while its strongest variety seems to be too thick – moral autonomy does not have to require that the agent should have the capacity to be motivated by moral considerations alone. However, I want to emphasize that, in my view, all the above varieties of autonomy are legitimate explications of the notion of autonomy. The formal variety of personal autonomy and the formal variant of the strong variety of moral autonomy seem to be just the best explications from among a number of legitimate explications, i.e., they seem to be explications that capture best the specificity of the concept of autonomy as it is used in the philosophical discourse.

Before I turn to the problem of the presuppositions of moral autonomy, I shall devote some attention to the problem of the relationships between these two concepts. Two different views of these relationships emerge. The first view states that they are entirely independent in the sense that an agent can be morally autonomous without being personally autonomous. This view leads to a rather counterintuitive conclusion that an agent's being entirely incapable of freely shaping and/or changing her first-order desires does not exclude her capacity to reflectively choose and/or reflectively affirm moral principles. According to the second view, the two concepts are partially dependent in the sense that an agent must be at least to some extent personally autonomous in order to be morally autonomous (to the same extent to which human agency presupposes personal autonomy, because moral autonomy presupposes human agency). This second view seems to be more plausible, because the capacity to

reflectively choose and/or affirm moral principles seems to require some level of the capacity to distance oneself from one's first-order desires.

## 2. *Presuppositions of autonomy*

What has been said so far – that there are two main concepts of autonomy, and that moral autonomy presupposes human agency ('being a true author of one's actions'), which, in turn, presupposes some level of personal autonomy – seems to be rather uncontroversial. What is controversial is whether moral autonomy has any other presuppositions and whether personal autonomy has any presuppositions at all. Before tackling these questions, let me clarify the concept of a presupposition of autonomy (used so far intuitively). Presuppositions of autonomy are conditions that must be satisfied in order to make sense of the concept of autonomy. They are therefore conditions which have to be met if one wants to speak of true rather than apparent autonomy. Accordingly, if a presupposition of a given concept of autonomy is not satisfied, the concept, so to say, falls apart: an agent who chooses her desires in a free way is only apparently personally autonomous, and an agent who chooses and/or affirms moral principles which are to govern her actions is only apparently morally autonomous. In short and less metaphorically, the notion of a presupposition can be equated with the notion of a necessary condition. This account of the notion of presupposition is general – it refers also to presuppositions of other notions than autonomy – for instance, to the notion of human agency, which strictly connected with the notion of autonomy. In the following two sections I shall argue that personal autonomy does not have any presuppositions, that it is not entirely clear whether human agency has two presuppositions (personal autonomy, free will) or three presuppositions (personal autonomy, free will, the contingency of birth), and – consequently – that it is not clear whether moral autonomy (which presupposes human agency) has two presuppositions or three presuppositions.

### a. Free will

Free will can be defined as the capacity to choose alternative actions in a given situation: an agent who has chosen an action at a given time has free will if she could have chosen some other action at that time. The question arises whether free will can be regarded a presupposition of personal or moral autonomy.

Personal autonomy requires that an agent have a second-order capacity to critically evaluate and to change her first-order desires. Now, there seems to be no connection between thus understood personal autonomy and free will. There seems to be no contradiction in assuming that an agent has the

above mentioned second-order capacity and does not have free-will, i.e., that she has the second-order capacity but all her thoughts, desires, actions are inevitable consequences of preceding events. In short, an agent can have the second-order capacity and simultaneously be deprived of free will. However, one may plausibly argue that even though free will is not a presupposition of personal autonomy, it is a presupposition of human agency. This is so because if an agent is deprived of free will, i.e., if her actions are just links in causal chains, then she can hardly be called 'an agent' – a *true* author of her actions. Accordingly, it seems plausible to maintain that human agency has (at least) two presuppositions – not only some level of personal autonomy but also free will. However, one could criticize this account of the relations between personal autonomy, free will and human agency by pointing out that free will *is* personal autonomy.<sup>2</sup> This explication of free will, though, seems to forfeit what seems to be an essential part of free will – the capacity to choose various options in a given situation, or, put alternatively, not being determined to choose a given option in a given situation. Accordingly, free will should be regarded as a presupposition of human agency, not as the presupposition of personal autonomy. Personal autonomy and free will should therefore be regarded as two *different* presuppositions of human agency.

Let me now turn to the question of whether free will is a presupposition of moral autonomy. Moral autonomy requires that an agent reflectively choose and/or affirm moral principles which are to govern her actions. Since the requirement that agent should reflectively choose and/or affirm moral principles implies that an agent should assume moral accountability for not complying with these principles, it can be said that moral autonomy implies moral accountability. And it can be plausibly argued that moral accountability for not complying with moral principles is justified only if the agent is not causally determined to act in a given way, i.e., if she has free will. Moral autonomy, therefore, presupposes free will. Clearly, one may argue for this just by pointing out that it is a direct consequence of the above account of the relations between personal autonomy, free will and human agency: given that some level of personal autonomy and free will are presuppositions of human agency, and that moral autonomy seems unthinkable without human agency, then moral autonomy presupposes free will (and some level of personal autonomy).

b. The contingency of birth

As we shall see, the question of whether the contingency of birth is a presupposition of human agency and thereby of moral autonomy is much

---

<sup>2</sup>Such explication of the notion of free will was put forward by Harry G. Frankfurt; see H. FRANKFURT, "Freedom of the Will", *o.c.*

more intricate than the question of whether free will constitutes such a presupposition. The claim that the contingency of birth is crucial for moral autonomy was put forward by Jürgen Habermas.<sup>3</sup> Habermas argues that our ethical self-knowledge as a species is grounded in the fact that our genetic constitution does not depend on the will of other persons, i.e., is contingent. What Habermas means by that is that a person cannot consider herself to be a real author of her actions and – more generally – of her life if she knows that other people decided about her genetic constitution. Accordingly, a person whose birth was not contingent cannot be expected to be able to take full responsibility for her actions, and thereby cannot be morally autonomous. Habermas's argument can therefore be plausibly construed as saying that the contingency of human birth is a presupposition of human agency. This argument is very profound – it seems to capture something really important about the nature of human agency and autonomy. However, it is not easy to articulate what exactly it captures and how it should be ultimately assessed. I shall start my analysis of Habermas's argument from a remark that if this argument is correct, it is not as self-evidently correct as the argument that some level of personal autonomy and free will are presuppositions of human agency. While it is (at least, in my view) self-evident that the possession of the second-order capacity to distance oneself from one's first-order desires (personal autonomy) and the capacity to have a real choice between various first-order desires (free will) are presuppositions of human agency, there seems to be nothing self-evident in the claim that human agency requires that a subject's genetic constitution should not have been designed by some other person. One might say that if a subject is personally autonomous and has free will, there seems to be nothing more needed to call her 'an agent'. Accordingly, it seems that the lack of contingency of birth does not by itself undermine human agency; it undermines it only in so far as it decreases personal autonomy beneath the 'threshold level' between agency and the lack of agency and/or violates her free will. Therefore, on this interpretation of human agency, contingency of birth is not a presupposition of human agency. Is therefore Habermas's claim that contingency of birth is a presupposition of human agency untenable? The matters are not so simple. There seem to be two main ways of defending this claim – one may call them 'philosophical' and 'psychological'. The philosophical way consists in pointing out that if we *really deeply* understand the concept of human agency as the concept of *true authorship* of one's actions, we cannot fail to notice that this concept requires the

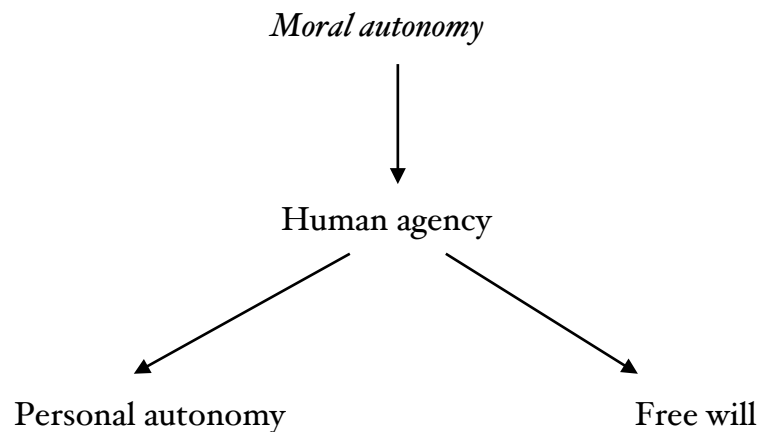
<sup>3</sup> See J. HABERMAS, *Die Zukunft der menschlichen Natur. Auf dem Weg zu einer liberalen Eugenik*, Frankfurt am Main, Suhrkamp Verlag, 2001. Habermas mentions that similar claim was made earlier by Hannah Arendt who (in *The Human Condition*) introduced the notion of natality as a pre-condition of human ability to initiate action.

contingency of birth; absent the contingency of birth, our authorship is not 'true', for the simple reason that we were designed not just by chance (which, on this argument, is a condition of our being true authors of our actions) but by some other person's conscious will. This way of defending Habermas's argument, however, encounters serious difficulties. First, one repeat the above made remark that the conception of human agency as based on personal autonomy and free will is sufficiently profound, so that there is no need to make it still 'more profound' by positing a somewhat obscure condition of the contingency of birth. Second, one may point out that, contrary to what Habermas seems to assume, the contingency of birth is an all-or-nothing notion. It is true that either a birth is contingent or not. However, it is also true that there is a fundamental difference between a negligent and substantial intervention in the embryo's genotype. On Habermas's view both types of intervention seem to undermine human agency to the same degree, while on the view that the contingency of birth is not a presupposition of human agency, they undermine human agency in varying degrees – depending on how they affect the presuppositions of human agency (personal autonomy and free will). The latter view seems more plausible. What's more, the view that the contingency of birth is a presupposition of human agency gives rise to a counterintuitive conclusion that an elimination of an embryo's genetic defects (i.e., negative genetic engineering) with a view to enabling the child's normal functioning as a human being undermines her agency (whereas, in fact, it would be right to say that it enables her agency). This counterintuitive conclusion can be avoided if we reject the claim that the contingency of birth is a presupposition of human agency. The psychological way of defending Habermas's argument, in turn, consists in asserting that a person who is aware that her birth was not contingent, i.e., that her genetic constitution was consciously shaped by other people, is unlikely to feel herself to be a true agent and thereby is unlikely to be able to reflectively choose and/or affirm moral principles which are to govern her actions, and, consequently, to accept moral accountability for compliance with these principles. One can respond to this argument by saying that this feeling of the lack of agency which an agent is likely to experience if she knows that her birth was not contingent can be eliminated by rationally arguing to her that the necessary and sufficient conditions of agency are personal autonomy and free will (or, if possible, by not revealing to her the information about the non-contingency of her birth). However, one could strengthen the psychological argument by claiming that such rational argumentation is not sufficient to eliminate this feeling, as this feeling is overwhelming, not open to rational argumentation about the bases of agency. Whether this feeling can be of such kind is an empirical question. In my view, it is rather implausible to maintain that it can. But even if it could, what would it show? Clearly, it would not show that contingency of birth is a

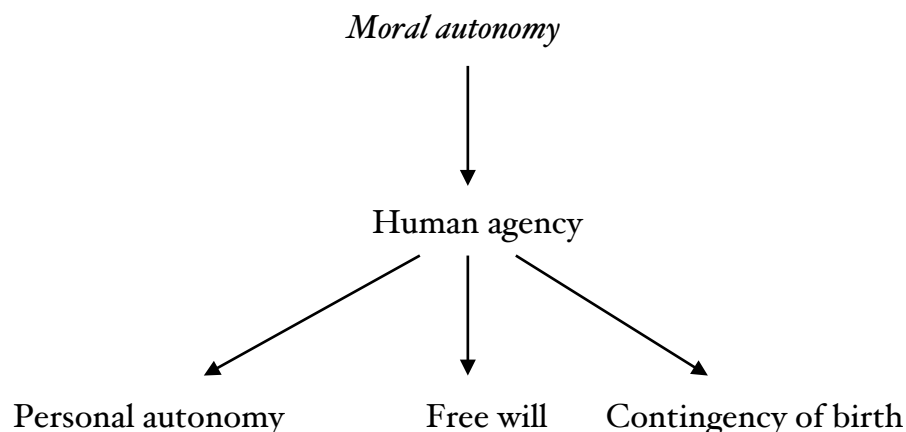
presupposition of human agency. It would only show that a person who knows that her birth was not contingent is likely to experience a difficulty with feeling herself the true author of her actions and thereby with taking full responsibility for her actions. But, let me repeat the point already made, by virtue of this fact the contingency of birth would not become a presupposition of human agency.

To sum up, the foregoing considerations seem to support the claim that contingency of birth is not a presupposition of human agency and thereby of moral autonomy. It is difficult, though, to provide a conclusive argument for this claim. Especially, it will be difficult to convince someone who just posits that the *profound* conception of human agency implies the contingency of birth. Therefore, given that it is not entirely clear what the presuppositions of human agency and thereby of moral autonomy are, one should distinguish two competing conceptions of moral autonomy (the arrows on the figures point to presuppositions of a given concept):

I.



II.



### III. GENETIC ENHANCEMENT

Before passing to the problem of whether genetic enhancement violates

human autonomy, it is necessary to distinguish two markedly different types of genetic enhancement (the distinction to be presented is widespread in the relevant literature<sup>4</sup>). The first type, which I call 'directed genetic enhancement', consists in that a decision-maker (e.g., parents) has an embryo's genotype modified in such a way that the embryo's development is strongly determined to proceed in a certain definite direction (i.e., a child is strongly determined to choose a given way of life wished by the decision-maker). The second type, which I call 'all-purpose genetic enhancement', consists in that a decision-maker (e.g., parents) has an embryo's genotype modified in a way that increases the embryo's overall capacities and powers to effectively pursue various life careers but does not determine the choice of any of those careers. Three additional remarks regarding the notion of genetic enhancement seem to be in order. First, when I speak of genetic enhancement and its influence on human autonomy, I mean a situation in which some decision-maker decides to enhance the nature of an embryo through genetic engineering, not just eliminate its defects that would preclude the embryo's normal functioning as a human being; I mean, then, positive, not negative, genetic engineering. Incidentally, it is worth noticing that negative genetic engineering does not seem to pose serious problems in the context of autonomy (unless, as mentioned, one assumes that contingency of birth is a presupposition of human agency): it enables a child's proper functioning of human beings, and therefore it enables her/his autonomy. Second, since the decision-maker may be – but does not have to be – the child's parents (the decision-maker may be, e.g., the state), the situation may take place both in the context of 'liberal eugenics' and in the context of 'authoritarian (state) eugenics'; the crucial point is only that some decision-maker decides to improve the other human being's – an embryo's – nature through genetic engineering. Third, an essentially different situation arises when a decision-maker uses genetic engineering to improve her own nature. In this situation genetic enhancement does not seem to pose any obvious threat to autonomy. It may be an expression of one's personal autonomy or not, depending on whether a subject has freely chosen her first-order desire to undergo a genetic improvement or not. And, depending on concrete effects of this improvement, it may diminish, increase, or leave intact her personal and moral autonomy.

---

<sup>4</sup>For a discussion of various aspects of genetic enhancement see, e.g., J. HARRIS, *Enhancing Evolution. The Ethical Case for Making Better People*, Princeton University Press, 2007; M. J. SANDEL, *The Case against Perfection. Ethics in the Age of Genetic Engineering*, Cambridge MA., Harvard University Press, 2007; P. VEZZONI, *Il futuro e il passato dell'uomo. Considerazioni sull'evoluzione umana*, Milano, Bruno Mondadori, 2006.

#### IV. DOES GENETIC ENHANCEMENT VIOLATE HUMAN AUTONOMY?

The answer to the question of genetic enhancement violates autonomy will depend on which conception of moral autonomy one accepts.

If one accepts the conception I of moral autonomy, then the answer will comprise the following theses:

- (1) Directed genetic enhancement diminishes personal autonomy. This is so because by determining an agent through genetic engineering to choose a concrete life career or at least to be capable of choosing from a smaller set of life careers than she would have been without the genetic intervention, one undermines the effectiveness of her second-order capacity to freely choose her goals. However, directed genetic enhancement does not have to affect moral autonomy. As argued, moral autonomy is only partially dependent on personal autonomy. Accordingly, the violation of personal autonomy will also be a violation of moral autonomy only if the violation of personal autonomy is so substantial as to make personal autonomy fall beneath 'the threshold level' between agency and the lack of agency.
- (2) All-purpose genetic enhancement does not diminish personal autonomy and does not affect in any way moral autonomy. *Au contraire*: all-purpose genetic enhancement increases a subject's personal autonomy, as it widens the range of goals from among which she can choose those goals she wishes to be *hers*.
- (3) If one accepts the conception II of moral autonomy, then the answer to the question of whether genetic enhancement violates autonomy will be composed of the following theses:
  - (1) Directed genetic enhancement diminishes personal autonomy (for the same reasons as it does on the grounds of the conception I of moral autonomy). Directed genetic enhancement violates moral autonomy, as it violates one of the presuppositions of human agency (and thereby of moral autonomy), namely, the contingency of birth.
  - (2) All-purpose genetic enhancement does not diminish personal autonomy but it violates moral autonomy (because it violates one of the presuppositions of moral autonomy, namely, the contingency of birth).

It should also be noted that irrespective of which conception of autonomy we accept, the following thesis holds: no type of genetic enhancement threatens the first presupposition of human agency – free will, since if one believes that humans possess free will, one will continue to do so, even if one knows that they are 'designed', not contingently born.

Clearly, for anyone for whom autonomy is an important value and who accepts the conception II of moral autonomy, the conflict between moral autonomy and genetic enhancement will be a strong argument against the admissibility of the genetic enhancement of embryos. However, as I have argued, the conception II of moral autonomy seems to be less plausible than the conception I. The preceding remark, though, does not imply that, if we accept the conception II of moral autonomy, genetic enhancement of embryos becomes admissible, because, apart from the argument from autonomy, one may advance many other arguments against genetic enhancement, not discussed in the paper.

**LET THEM BE PEERS:  
THE FUTURE OF P2P SYSTEMS AND THEIR  
IMPACT ON CONTEMPORARY LEGAL NETWORKS**

Ugo Pagallo\*

**I. INTRODUCTION**

The subject of this paper – “the future of P2P systems and their impact on contemporary legal networks” – requires three preliminary elucidations.

First, it does not rely on any prophetic powers or divinatory commitments; rather, the aim is to draw attention to some major issues concerning today’s P2P systems. By highlighting these problems, the idea is to specify possible developments and changes induced by technology.

Secondly, I look at file sharing application-systems and not at social networking on the Web 2.0. Peer production, among other things, has created and continues to raise new interesting cases in contemporary legal networks. Here, I only consider peer interaction mediated by P2P systems because this strict limitation allows me to focus on more precise targets.

Finally, the study of the impact of P2P systems on contemporary legal networks is not blind to the reciprocal interaction between technology and the law. On the contrary, I will stress how legislators and courts often shape (or try to influence) the evolution of technology. All in all, P2P systems are excellent examples for such a bidirectional connection between technical evolution and social environment.

Following these premises, this paper is presented in four parts.

The first part on “P2P and legal systems” is divided in three sections. In section A, I illustrate the way in which technology has changed contemporary legal systems in complex and often unpredictable manners, and how legislators (and courts) have responded to such transformations. In the case of P2P systems, the price of success has been high: a determined and even aggressive protection of copyright holders against “peer-to-peer” file sharing application-systems that make it easy for the Internet users to obtain items for free.

In section B, I examine this new crusade by looking at some well-known

---

\* Full Professor in Philosophy of Law at the Faculty of Law, University of Turin.

cases like *Napster*, *Grokster*, and *Elektra v. Baker* from 2008. The trend is such that some politicians in Washington (D.C.) like the Government Reform Committee Chairman, Henry Waxman (D-CA), Rep. Tom Davis (R-VA), and Rep. Paul Hodes (R-NH), have even argued the technology used in P2P systems represents a serious problem for national security!

In section C, I notice however that things are recently changing, at least, in Europe. In fact, P2P systems do not only concern matters of copyright, but of privacy as well. Copyright protection is not reason enough to carry out extremely invasive monitoring techniques. The European Court of Justice's decision in *Promusicae v. Telefónica de España* (C-275/06) shows that "a fair balance [has] to be struck between the various fundamental rights protected by the Community legal order."

Hence, by adopting this latter perspective, it is possible to address both threats and opportunities of P2P systems in a well-balanced way, so that today's issues and persisting problems help casting light on tomorrow's developments.

In part III, I explain why I disagree with scholars who claim that hubs or Super-peers are unessential to P2P systems inasmuch as these systems would be only distributed networks, that is systems where "authoritative nodes" may exist but are not necessary as in the Internet.

In part IV, I deepen some technical solutions which have been proposed and discussed by both legal experts and computer scholars, in order to cope with some of the most relevant issues on the political agenda.

The conclusion is that time has come to leave behind some exaggerations in the current debate: P2P systems are not a menace or risk that should simply be banned or shut down, and they are not the key to a new egalitarian paradigm that has to be encouraged as such. Rather, by analyzing the future of these systems it is important to insist on the mutual interaction through which technology is reshaping both legal concepts and their environmental framework, while political decisions influence or attempt to determine the development of technology. Following this fruitful third way, the aim is to show why it is so important to let peers be and evolve.

## II. P2P AND LEGAL SYSTEMS

### I. *The price of success*

The ICT revolution has changed contemporary legal networks in, at least,

three different ways.

First, technology has deeply transformed the approach of experts to legal information as it occurs, say, with documental legal informatics, e.g., information retrieval and legal databases.<sup>1</sup> Furthermore, computer science sheds new light on such traditional areas as jurisprudence and legislation insofar as electronic maps of their topological structure can be made, according to specific laws of informational distribution.<sup>2</sup>

Secondly, technology has induced new kinds of lawsuits, or has radically modified old forms. On one side, it is enough to mention some new types of offences such as computer crimes; on the other side, technology has also changed traditional rights such as privacy (1890) and copyright (1710), both turned most of the times into a matter of access, control, and protection over information in digital environments.<sup>3</sup>

Finally, technology has blurred conventional national boundaries as information on the Internet tends to have an ubiquitous nature that transcends traditional legal borders and questions the notion of the law as made up of commands enforced through physical sanctions. Spamming, for instance, is a good example: It is *par excellence* transnational and does not seem to diminish despite severe criminal laws (as the *CAN-SPAM Act* approved by the U.S. Congress in 2003).

This undeniable impact of the ICT revolution has however led to some misunderstandings: One misconception concerns the idea that technology is something neutral, another is that legislators (and courts) cannot influence the development of technology. As far as the first error is concerned, technology would only be a means for whatever end, regardless of good or evil; in the second case, technology would be too swift and powerful to be effectively limited by the slow pace of law-making and jurisprudence.

Yet, this picture is incomplete since it omits to stress how deeply technology modifies the ways in which scholars address most of their legal issues and, vice versa, how legal systems influence the architecture of

---

<sup>1</sup> A good introduction in G. SARTOR, *Corso d'informatica giuridica*, vol. I: *L'informatica giuridica e le tecnologie dell'informazione*, Torino, Giappichelli, 2008.

<sup>2</sup> Cf. U. PAGALLO, "Small world" Paradigm and Empirical Research in Legal Ontologies: a Topological Approach, in *The Multilanguage Complexity of European Law: Methodologies in Comparison*, edited by G. Ajani, G. Peruginelli, G. Sartor, and D. Tiscornia, European Press Academic Publishing, Florence 2007, pp. 195-210.

<sup>3</sup> Further details in U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Milano, Giuffrè, 2008.

digital environments. This is precisely what happens with copyright: Law-makers react both to changes and challenges brought on by technological evolution as they mould or try to shape such a development via the law and its applications. So, the more relevant a technology is in terms of innovation speed, transformation, and social impact, the more it is likely policy-makers and courts will intervene.

This straight correlation is just the legal price of technological success and it is confirmed by several cases involving privacy, computer crimes, and of course, P2P systems-related copyright issues.

Here, a brief account of this trend over the last ten years suffices: In 1998, the U.S. Congress approved the *Digital Millennium Copyright Act* (DMCA) and the so-called *Sonny Bono Act*; three years later, the European Parliament and the Council adopted the first EU directive on “copyright and related rights in the information society.” Then, the U.S. Congress passed the *Consumer Broadband and Digital Television Promotion Act* in 2002, the *Family Entertainment Copyright Act* in 2005, and the *Net Neutrality Bill* in 2006. Meanwhile, the IPRED saga developed in Europe: the first directive on the enforced intellectual propriety rights is from 2004 (n. 48), and on April 25<sup>th</sup>, 2007, the European Parliament supported a new version (IPRED-2).

In a nutshell, this legal outline confirms the twofold process mentioned above: As technological progress reshapes key assumptions in legal arguments, legislators react to this by favouring certain technical and political choices over others. While technology transfigures the essence of traditional copyright issues – since there is no longer any theoretical difference between original and copy – law-makers have generally overreacted to this revolution. It seems that the second comma of art. 27 of the Universal Declaration of Human Rights – i.e., “the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author” – simply prevails over the first one, stating “the right freely to participate in the cultural life of the community, to enjoy the arts and to share in scientific advancement and its benefits.”

In order to explain this trend, let me go back to the realm of P2P systems: Indeed, these file sharing application-techniques were developed from the late 1960s onwards, but they became extremely popular only in the late 1990s, *et pour cause*, with the legal misadventures of Napster. Again, we witness the legal price of technological success.

## 2. *Copyright crusaders*

The first important decision on copyright and P2P systems came in July 2000, when the U.S. District Judge Marilyn Patel granted the *Recording Industry Association of America* (RIAA)'s request to stop making copyrighted recordings available for download through Napster services. Although the San Mateo company did not store any information, such as the recordings on its own computers, it was declared illegal to provide the information of where the songs were available on the computers of the community logged on. In other words, it was not considered enough to claim that the DMCA grants immunity to ISP providers for what their customers do. As a matter of law, this kind of protection would not include "contributory infringers" as the District Court of Appeals confirmed in its own decision on Napster, in February 2001.

(Later on, I insist on how this wave of mandatory assessments suggested the next generation of P2P systems to adopt a more massively distributed way of spreading and exchanging information on the Internet. In fact, Napster's centralized architecture meant that operators of the central server used to index each peer's files and, hence, they could have intervened to stop copyright infringements pursuant art. 512 of the DMCA. For the moment, it is sufficient to stress the relevance of these first verdicts on Napster, insomuch as they confirm the abovementioned twofold process: Technological progress reshapes some key legal issues of contemporary networks while law-makers and courts react to this evolution by favoring certain choices over others.)

Four years later, in 2005, it was the turn of the U.S. Supreme Court in *MGM v. Grokster* to present P2P systems as Steamcast or Grokster, as a kind of technology that promotes the "ease of infringing on copyrights," so that its producers "can be sued for inducing copyright infringement committed by their users." Notwithstanding this unanimous holding by the Court, the legal consequences on further developments of P2P technology remained however unclear. Indeed, the Supreme Court justices were divided between the need to protect every technology "capable of substantial non infringing uses" as they declared in *Sony v. Universal City Studios* from 1984, and the necessity to provide remedies against new ways of copyright infringement.

So far, in the U.S., the problem remains to determine whether the software creates "shared files folders" making the very information protected by copyright "available for distribution" and hence illegally shared via those "files folders." In *Elektra v. Baker*, for example, a judge from the Manhattan federal court, Kenneth Karas, rejected the RIAA's "making available"-

theory in January 2008, even if he admitted the sufficiency of the allegations of “downloading” and “distributing,” thereby giving the RIAA an opportunity to reformulate its pleadings. Whereas Karas’ idea is to grasp the whole issue with the legal hypothesis of “offering to distribute for purposes of redistribution,” it seems more fruitful to note how the suit in *Elektra v. Baker* was based on a report of an Internet investigator who claimed to have detected the “shared files folders” which I presented above.

In fact, there is a second major legal issue, besides copyright, that involves P2P systems and their technological evolution: that is privacy. As it occurred with another highly controversial decision in the U.S. opposing an American ISP, Verizon, and the RIAA again, scholars have pointed out “how the privacy of Internet users participating in P2P file-sharing practices is threatened under certain interpretations of the Digital Millennium Copyright Act (DMCA) in the United States [as] a new form of ‘panoptic surveillance’ that can be carried out by organizations such as the RIAA.”<sup>4</sup>

The thesis was confirmed in 2007, when the *Motion Picture Association of America* (MPAA) required (lawfully, according to federal judge Florence-Marie Cooper) the IP addresses of those connecting to TorrentSpy files via their service in the U.S. The MPAA had in fact filed a lawsuit against the popular P2P system, alleging that the company violated copyright law by helping sharers find pirated movies.<sup>5</sup> The dispute then overheated when TorrentSpy accused the MPAA of hiring a hacker (by the way an ex TorrentSpy employee) in order to pilfer the company’s trade secrets. Judge Cooper’s interpretation, however, did not favour the European company: in the name of the *Wiretap Act*, the word “intercept” would only mean that someone must intentionally intercept e-mails and not just acquire them from an electronic storage. Therefore, since TorrentSpy used to store e-mails on its server before they were copied and forwarded to the hacker’s e-mail account, the result was that no interception would have occurred! Forced to enable server logging against its own privacy policy, it is not a surprise that TorrentSpy, whose servers are physically located in the Netherlands, announced its decision to stop doing business in the U.S. on August 27<sup>th</sup>, 2007.

---

<sup>4</sup> The thesis in F. S. GRODZINSKI, H. T. TAVANI, “P2P Networks and the Verizon v. RIAA case: Implications for personal privacy and intellectual property”, *Ethics and Information Technology*, 7, 4, pp. 243-250.

<sup>5</sup> Cf. U. PAGALLO, *La tutela della privacy*, o. c., pp. 230-231.

### 3. *Privacy concerns and fundamental rights*

Legal troubles of P2P systems with both copyright and privacy issues illustrate some peculiarities of the U.S. legal system as well as some key differences between U.S.- and EU-law. If a property standpoint prevails in the former legal system, privacy is widely considered as a fundamental right in the latter, proclaimed both by the European Convention from 1950 and the EU Charter of Nice in 2000, let aside the specific constitutional traditions of Member States. In order to understand this hiatus and, thus, the different ways in which legal frameworks affect the evolution of technology, it suffices to recall two cases recently discussed in Europe.<sup>6</sup>

The first one took place in Italy in 2006, when a German music company, Peppermint, commissioned the Swiss firm Logistep to raise the IP addresses of people making available copyrighted works by means of P2P systems on the Internet. On the basis of the claim that Peppermint would have been the only right holder, the plaintiff required a section of the Tribunal in Rome to obtain both the “real addresses” and names of 3000 suspected illegal file sharers from the involved ISPs. At first, judges granted the request so that three thousands letters were sent by a lawyer from Bozen to the indicted P2P users, asking them for EUR 330 in order to settle the case and avoid any further inquiry. (In this way, Peppermint would have received cash worth almost ten times its own annual revenues...) Later on, in April 2008, the Bar Association of Paris interdicted a lawyer who sent similar letters to French P2P users. However, even the Tribunal in Rome changed idea: In fact, on June 16<sup>th</sup>, 2007, it declared that spying citizens on the Web in order to guarantee the protection of alleged copyrights holders pursuant articles 13, 23, and 37 of the Italian “code of privacy” (ICP) as well as articles 2 and 15 of the Italian Constitution, was illegal. Neither articles 8 and 9 from D-2004/48/EC, nor the exceptions from articles 3.2 and 13 D-1995/46/EC, could eventually legitimate such a violation of P2P users’ privacy.

Yet, there is another important ruling that confirms the relevance of data protection laws in deciding lawsuits against P2P file sharing systems. The case is *Promusicae v. Telefónica de España*, decided by the European Court of Justice on January 29<sup>th</sup>, 2008. According to the judges in Luxembourg, the EU law does *not* require Member States to lay down “an *obligation to communicate personal data* in order to ensure effective protection of copyright in the context of civil proceedings.” In addition, the Court warned that, when transposing directives into national legal systems, Member States must “take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights

<sup>6</sup> More details in U. PAGALLO, *La tutela della privacy*, o.c., pp. 232-234.

protected by the Community legal order.”<sup>7</sup>

The ECJ decision, however, is problematic for the following reasons.

First, it does not mean that a national provision is incompatible with EU law because it obliges ISPs to disclose the identities of their subscribers for alleged violations of copyright law.

Secondly, the final output of such a “fair balance to be struck between the various fundamental rights,” protected by any western-like legal order, is far from clear.

Even so, the ruling has the merit of highlighting that P2P systems do not only involve private claims on copyright infringements, but also privacy concerns about data protection in digital environments. Whereas legal scholars in the U.S. still discuss the possibility to ascertain whether P2Ps are a technology capable of substantial non infringing uses, it is clear that, at least in Europe, such a copyright protection must go along with the fair respect of P2P users’ personal data. Although these systems have become infamous as file sharing applications that make it particularly easy for users to access copy(right)-protected files for free, the problems arisen cannot be resolved simply by banning this technology from campuses, schools, military areas, and the like. Indeed, you need not be an advocate of this technology or of Yochai Benkler’s ideas on “peer production” to recognize that people are creating, via P2P systems, brand new ways of producing and distributing goods via networks that are of cooperative nature and that are highly decentralized;<sup>8</sup> that is, networks that have been embraced even by colossuses like IBM. So, it is time to show why it is important to let them be peers.

### III. THEORETICAL PERSPECTIVES: A TOPOLOGICAL APPROACH

The new generation of strongly decentralized and encrypted P2P architecture that provides plausible anonymity for its members, is actually producing new problems and original forms of uncertainty, compared to those deriving from the first generation of weakly decentralized systems in which the origin and destination of information could be traced with relative ease. However, the sophisticated post-Napster generation – from Gnutella’s unstructured P2P system to KaZaA’s decentralized one – should

---

<sup>7</sup> E.C.J., Case C-275/06, *Promusicae v. Telefónica de España*, 2008/C 64/12, § 70.

<sup>8</sup> On the very notion of “peer production” see Y. BENKLER, *The Wealth of Networks. How Social Production Transforms Markets and Freedom*. New Haven, CT., Yale University Press, 2005.

not be criminalized. Despite numerous problems like security and privacy, copyright and connectivity issues, and the free riding phenomenon, P2P systems offer means for optimizing the distribution of information in complex social networks and they have surpassed the Web as the single most bandwidth-consuming application in many parts of the Internet today.

Thus, it is not hard to understand why it is crucial to address the topic of the future of P2P systems: It involves tomorrow's Internet as well as some of the main issues of contemporary legal networks. Let me start here with some theoretical remarks.

First of all, the horizontal architecture of P2P systems has created wider opportunities, both in scope and quantity, for the production and distribution of information on the Internet. Furthermore, scientific papers have shown the existence of spontaneous clustering of users, according to content which is distributed in P2P networks such as Gnutella or KaZaA. These "small world" properties have been detected via different methods as the "data sharing graphs",<sup>9</sup> or the "affinity networks".<sup>10</sup> The typical high clustering coefficients go along with short diameter networks thanks to the performance of hubs, as in other complex networks like the Internet, the Web, telephone graph calls, scientific quotations as well as the structure of both the U.S. Congress and the Swedish Parliament. Indeed, many complex networks present these very features of "small worlds" – high clustering, short diameter, and presence of hubs – because the distribution of information is spontaneously optimized in this way by complex systems.<sup>11</sup>

This effect of "rich gets richer" has suggested some scholars to claim that hubs or Super-peers are actually unessential as proper P2P systems would be only distributed networks, that is systems in which "authoritative nodes" may exist but are not necessary as it occurs with the Internet.<sup>12</sup>

<sup>9</sup> As in A. IAMNITCHI *et al.*, "Small-world file-sharing communities" in the 23<sup>rd</sup> Conference of the IEEE Communications Society. Hong Kong, InfoCom, 2004.

<sup>10</sup> As in G. RUFFO, R. SCHIFANELLA, "A Peer-to-Peer Recommended System Based on Spontaneous Affinities", in *Technical Report RT 96/06*, Dept. of Computer Science, University of Turin, 2006.

<sup>11</sup> Cf. U. PAGALLO, *Teoria giuridica della complessità. Dalla polis primitiva di Platone ai mondi piccoli dell'informatica: un approccio evolutivo*, Torino, Giappichelli, 2006.

<sup>12</sup> This is the thesis of M. BAUWENS, *P2P and Human Evolution. Placing Peer to Peer Theory in an Integral Framework*. On line at <http://integralvisioning.org/article.php?story=p2pththeory1> (the paper is from 2005; last checked on Nov. 26, 2008)

However, the assumption rests upon utopian visions of pure egalitarian relationships, missing the crucial connection that emerges from a topological viewpoint: The “long tail” of information with the “rich gets richer”-effect – characterized by few nodes with very high values, and by most nodes with small degree – has to be seen in light of the clustering coefficients of the network. If these coefficients are low, we have a simple random network, i.e., a kind of network that illustrates some of the main criticism to current globalisation for hubs would have an anti-democratic nature as it was stressed by Barabási.<sup>13</sup> But, if these coefficients are high, local gathering of the nodes suggests that hubs which reduce the diameter of the network are indeed useful and justifiable. After all, what P2P systems obtain spontaneously on the Internet, is precisely what contemporary globalisation lacks: self organized-based clusters of users evolve together with hubs that shorten the diameter of the network.<sup>14</sup>

Besides, it is a matter of fact that most P2P systems *still* present hubs: Namely users who share a large amount of items, thereby playing a main role in providing connectivity. Such a “small world” feature of the system is in fact rather crucial as it has been exploited to obtain both new recommendation systems on the Web and new methods for attacking, say, copyright infringements. In the first case, by exploiting the high clustering coefficients of the network – its “affinity circles” along with its transitive properties – it becomes feasible to recommend information without requiring personal data as hubs can be seen as vectors for developing all the opportunities offered by this technology.<sup>15</sup> In the second case, hubs may be conceived, on the contrary, as targets in order to break these systems and, therefore, the relative emerging communities of digital affinity.<sup>16</sup>

The panoply of possible applications, pro or contra privacy, pro or contra copyright, does not imply, of course, that technology should be considered once again as “neutral,” i.e., a means to obtain whatsoever end. Rather, it is

<sup>13</sup> The classical text is of course A.-L. BARABÁSI, *Linked. The New Science of Networks*. Cambridge, Mass., Perseus, 2003.

<sup>14</sup> Cf. U. PAGALLO, “‘Small World’ Paradigm in Social Sciences: Problems and Perspectives”, in *Glocalisation: Bridging the Global Nature of Information and Communication Technology and the Local Nature of Human Beings*, edited by T. Ward Bynum, S. Rogerson, and K. Murata, e-SCM Research Center and University of Meiji, Tokyo, 2007, pp. 456-465.

<sup>15</sup> As shown by G. RUFFO, R. SCHIFANELLA, “Efficient Profit Sharing in Fair Peer-to-Peer Market Places”, *Journal of Network and System Management*, 15(3), pp. 355-382.

<sup>16</sup> As discussed in U. PAGALLO, G. RUFFO, “On the Growth of Collaborative and Competitive Networks: Opportunities and New Challenges”, in *Ethicomp Working Conference 2007*, edited by S. Rogerson e H. Yang, Yunnan University, 2007, pp. 92-97.

crucial to insist on the mutual interaction through which technology reshapes both legal concepts and their own environmental framework, while political decisions influence or attempt to determine possible developments of technology. After some theoretical remarks on new feasible horizons of P2P networks, it is now necessary to look at their future through some more technical lenses.

#### IV. A FAIR BALANCE FOR NEW DEVELOPMENTS

In the summer of 2008, Andrea Glorioso, Giancarlo Ruffo, and I were working on a chapter for a Springer book on P2P systems, analyzing the topic of their “social impact.” In fact, while hundreds or even thousands of papers and dozens of meetings focus on technical developments of those systems, they rarely couple their research with the societal boundaries which limit or restrict the universe of possible extensions for such an evolution. What about the consequences of the Grokster case in light of that “fair balance” to be struck between fundamental rights, according to the ECJ ruling in *Promusicae v. Telefónica*?

Let me sum up some of our conclusions in the forthcoming chapter by considering new ways of sharing and distributing information in digital environments. I take into account three of these.

First, it is well-known how users, within P2P systems, turn out to be “servents,” i.e., both clients and servers, or “prosumers,” namely producers and consumers at the same time. Hence, boundaries between owners and providers, distributors and consumers, are becoming increasingly blurred as owners do not always coincide with providers. Therefore, technical solutions for the next generation of P2P systems will not only need to cope with dependable and scalable models, but also with plain revenues for owners and ways for sharing profits with providers or mediators such as banks, credit card companies, brokers, or certification authorities.

Second, the structured vs. unstructured P2P systems-debate should be reformulated in legal terms: At an overlay level, indeed, structured models seem preferable in order to prevent legal claims as liability for actions committed by users of these systems. Further, compared to centralized systems, such structured overlays do not seem to present single points of failure or problems of efficiency as the flooding search method adopted by Gnutella. Besides, they do not push legal responsibility over few super-peers as it occurs with KaZaA.

Third, privacy must be accounted for as well: Both anonymity and confidentiality in P2P interaction should be addressed at the lowest level

of the technological platform since using the overlay network makes it possible to easily identify users inserting or storing information in the system. Authentication protocols as well as identification policies should provide for use of pseudonyms, OpenID, and ways of ciphering content. In this way it is safer to prevent not only unauthorized access to the information stored at the overlay level, but also legal liability of the content provider whom does not happen to be the source or the owner of that very information.

Of course, anonymity and confidentiality techniques, along with ways of encrypted communication, can be used by criminal organizations as well: All in all, it is still a debatable question whether OpenID solutions represent the ultimate way to solve these issues. In any case, it is certain that, among other things, 'al Qaeda has been using encryption since 1993, that is in their first and partially failed attack on the Twin Towers.<sup>17</sup>

Again, this does not mean technologies as P2Ps are something "neutral." On the contrary, it must be stressed how developments of such techniques are transforming key concepts of current legal and political debate – as it clearly occurs with notions of copyright, privacy, security, and the like – while law-makers, courts, and scholars attempt to tell fair and lawful practices from unlawful activities.<sup>18</sup>

Indeed, societal constraints determine the horizon of possible technological improvements which influence, at the same time, the evolution of contemporary legal networks. What is at stake, in both cases, is the way information is created, distributed, and shared in digital environments, according to that "fair balance" that must be struck between fundamental rights. From a technical viewpoint, it is essential to cope with issues of connectivity, availability of resources, and system performances in order to optimize flow of information within a given system. Hence, in the legal field, scholars should take into account the ways in which copyright has changed in a world of servants and/or prosumers, privacy has been deeply modified by new techniques of data protection and aggression in the informational age, security is challenged by new powerful tools of encryption and anonymity, up to the general

---

<sup>17</sup> Cf. A. ETZIONI, *How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism*, New York-London, Routledge, 2004, p. 35.

<sup>18</sup> See again U. PAGALLO, *La tutela della privacy, o.c.*, pp. 10-12; and my paper "Ethics Among Peers: From Napster to Peppermint, and Beyond", in the 5<sup>th</sup> *itAIS Conference on "Challenges and Changes: People, Organizations, Institutions and IT"* organized by the Italian Association for Information Systems in Paris, France, on Dec. 13-14, 2008, at <http://eventseer.net/e/7947/> and to be published by Springer, 2009

remarks I did introducing part II.

Such a bidirectional connection between technology and the law, in which one affects or feedbacks the other in a continuous cycle, brings us back to some popular exaggerations in current debate. In the introduction, I recalled some politicians in Washington, who claim the only way to solve P2P problems would be to simply ban them or shut them down; in part III, on the contrary, I mentioned scholars who interpret these systems as a sort of new paradigm which should be encouraged as such. The need to tell fair from unlawful outcomes is a good way to leave behind such overstatements: It is time to draw some conclusions.

## V. A NORMATIVE CONCLUSION

Throughout these pages, I have pointed out that debate on P2P systems can be summarized in two extreme positions. Some scholars, like Michael Bauwens, claim that P2P technology represents the key of a new paradigm insofar as sharing of information via strongly decentralized or distributed forms of coordination among geographically dispersed actors would be the paramount example of a deep social transformation that should be further encouraged.<sup>19</sup> Others, on the contrary, as Andrew Keen, stress risks and threats of new technologies and how they undermine vital elements of our societies for “digital piracy, enabled by Silicon Valley hardware and justified by Silicon Valley intellectual property communists [sic!] such as Lawrence Lessig, is draining revenue from established artists, movie studios, newspapers, record labels, and song writers.”<sup>20</sup>

However, it is not so difficult to show limits and faults of both viewpoints.

On the side of the new paradigm-advocates, it is enough to mention some of the serious problems afflicting P2P technology as security and privacy threats, copyright claims, issues of connectivity, availability of resources, and, to be pessimistic in some cases, even the collapse of the system.

On the side of P2P censors and opponents, vice versa, it should be stressed both the vitality and strength of these file sharing application systems that, optimizing how information is distributed and shared by their peer users, have created wider opportunities in digital environments.

---

<sup>19</sup> See again M. BAUWENS, *P2P and Human Evolution*, *supra* note 12.

<sup>20</sup> A. KEEN, *The Cult of the Amateur. How Today's Internet is Killing Our Culture*, New York, Doubleday, 2007, quoted by D. TAPSCOTT, A. D. WILLIAMS, *Wikinomics. How Mass Collaboration Changes Everything*, London, Portfolio (Penguin), 2008, p. 273.

In any case, it is not a simple matter of equalizing the exaggerations of both sides: On the contrary, my thesis is that most of the challenging issues come from the latter side for a couple of reasons.

The first point is cynical: Most of the times, critics and detractors of P2P systems are not simply scholars but powerful politicians and lobbyists, who have played a major role in passing the increasing amount of law as those illustrated in parts I and II.

The second reason is theoretical: Ideas sponsored by advocates of the new paradigm can be fairly confuted by experience, but the reverse is not true in case of a ban. Actually, interventions for reducing potential risks of P2P systems would be carried out until the thesis is finally proven to be false. Nevertheless, full validation of that thesis, i.e., P2P systems are too risky so they should be banned, cannot be satisfied due to the early imposition of that ban!<sup>21</sup>

So, how can we prevent such a deadlock? How can we convince P2P detractors that the main task is not to shut them down but, rather, to further develop them?

One way is to remind policy-makers of the real essence of an open society, say, in the wake of Karl Popper, Friedrich Hayek, or according to supporters of contemporary digital openness as Lawrence Lessig.<sup>22</sup> Still another possibility is to insist on the strict link P2P technology has with open source approaches, peer production, and collaborative models, which are transforming today's economy and social relationships.<sup>23</sup> In this latter case, it is not hazardous to predict how prohibitionist legislations will only have a short breath, while in the former case it is likely that the next crucial legal issue would be freedom of research.

(In fact, another way to grasp the point is to reconsider it via an evolutionary approach. That means, in informational terms, that any attempt to adapt to the environment has to reduce its complexity, e.g., the aim of P2P systems to avoid the noise while optimizing the distribution and sharing of information on the Internet. But, in doing so, it is still an

---

<sup>21</sup> See U. PAGALLO, *Something Beyond Technology: Some Remarks on Ignorance and Its Role in Evolution*, in *Living, Working and Learning Beyond Technology*, edited by T. W. Bynum, M. C. Calzarossa, I. De Lotto e S. Rogerson, Tipografia Commerciale, Mantua, 2008, pp. 623-631.

<sup>22</sup> Cf. L. LESSIG, *The Future of Ideas. The Fate of the Commons in a Connected World* [2001], New York, Vintage Books, 2002.

<sup>23</sup> An overview in Ch. ANDERSON, *The Long Tail. Why the Future of Business Is Selling Less of More*, New York, Hyperion, 2008.

open question whether such informational reduction enriches the complexity of the whole or, rather, diminishes it. For example, it is obvious that P2P opponents think these systems fall within the latter case as it is confirmed by hypotheses of copyright infringement and threats to creativity and innovation which deserve to be shut down. Yet, there is a lot of evidence that shows how P2P systems do improve the informational complexity of the whole: let aside means of distribution and sharing, think of all the old songs people discover on the Web that even their copyright holders had forgotten in their catalogues! Therefore, what is required in order to cope with the undeniable problems of P2Ps is not to shut them down. Rather, further research is needed: Q.E.D.)

So, the future of P2P systems can be summarized in three final remarks.

*First*, it is quite likely that the single most bandwidth-consuming application of the Internet will be increasingly improved by experts, trying to resolve issues like availability of resources, connectivity, the free riding phenomenon, and the overall system performance. From this viewpoint, you need not follow Friedrich Hayek's thesis on the complexity of *cosmos* and how spontaneous orders overrule human plans (*taxis*) to foresee the shortcomings of attempts to stop both the economical and sociological trends mentioned above.

*Second*, the future of P2P systems has to be considered in connection with the necessary restraints imposed by a (wise) set of legal rules as discussed in this paper. While changing the very way in which scholars debate on some crucial topics as copyright, privacy, or security, the evolution of P2P systems is entwined with new forms of intending what is right (to information) in digital environments. Once again, against the short-minded motives of P2P opponents, it is more a matter of research and scientific evidence than of ideology.

*Third*, this evolution highlights the mutual feedback between technology and the law, i.e., the thread of Ariadne in this paper and object of a conclusive remark. The state-of-the-art in today's research is not able to predetermine, with any likelihood, the mutual conditioning of P2P systems and the key legal issues dealing with them. However, from the normative viewpoint, what we ignore today also teaches us how to construct the work of tomorrow. Despite threats and risks of P2P systems, significant evidence suggests that this technology enriches human interaction by opening ways of sound collaboration, creative relationships, and participation "in the cultural life of the community." In the name of the Universal Declaration of Human Rights, we should therefore let them be peers.