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

1. *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.[1] 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.[2]

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.[3]

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 misconstruction 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

---

[1] A good introduction in G. SARTOR, *Corso d'informatica giuridica*, vol. I: *L'informatica giuridica e le tecnologie dell'informazione*, Torino, Giappichelli, 2008.

[2] 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.

[3] 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 25th, 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."[4]

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.[5] 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 TorrentySpy 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 27th, 2007.

---

[4] 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.

[5] 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.[6]

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 16th, 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 29th, 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

6 More details in U. PAGALLO, *La tutela della privacy*, *o.c.*, pp. 232-234.

protected by the Community legal order."[7]

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;[8] 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

---

7 E.C.J., Case C-275/06, *Promusicae v. Telefónica de España*, 2008/C 64/12, § 70.

8 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",[9] or the "affinity networks".[10] 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.[11]

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.[12]

---

[9] As in A. IAMNITCHI *et al.*, "Small-world file-sharing communities" in the *23rd Conference of the IEEE Communications Society*. Hong Kong, InfoCom, 2004.

[10] 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.

[11] Cf. U. PAGALLO, *Teoria giuridica della complessità. Dalla polis primitiva di Platone ai mondi piccoli dell'informatica: un approccio evolutivo*, Torino, Giappichelli, 2006.

[12] 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=p2ptheory1 (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.[13] 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.[14]

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.[15] 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.[16]

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

---

[13] The classical text is of course A.-L. BARABÁSI, *Linked. The New Science of Networks*. Cambridge, Mass., Perseus, 2003.

[14] 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.

[15] 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.

[16] 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.[17]

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.[18]

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 servents 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

---

[17] Cf. A. ETZIONI, *How Patriotic Is the Patriot Act? Freedom versus Security in the Age of Terrorism*, New York-London, Routledge, 2004, p. 35.

[18] 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 *5th 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.[19] 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."[20]

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.

---

[19] See again M. BAUWENS, *P2P and Human Evolution*, *supra* note 12.

[20] 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![21]

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.[22] 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.[23] 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

---

[21] 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.

[22] Cf. L. LESSIG, *The Future of Ideas. The Fate of the Commons in a Connected World* [2001], New York, Vintage Books, 2002.

[23] 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.