LAWYERS *in the* MEDIA SOCIETY

The Legal Challenges of the Media Society

Edited by

Ahti Saarenpää and Karolina Sztobryn

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND

Faculty of Law
and Administration

University of
LODZ

Lawyers in the Media Society.
The Legal Challenges of the Media Society

Edited by Ahti Saarenpää and Karolina Sztobryn

LAPIN YLIOPISTO
UNIVERSITY OF LAPLAND
ROVANIEMI 2016

This book is a result of the collaboration between:

University of Lapland, Faculty of Law, Institute for Law and Informatics
and
University of Lodz, Faculty of Law and Administration

Layout and editing Ahti Saarenpää and Karolina Sztobryn
Reviewed by Erich Schweighofer
Cover design Aleksander Wiatrowski

ISBN 978-952-484-908-1
ISBN pdf 978-952-484-913-5

University of Lapland Printing Centre
Rovaniemi 2016

Content

Introduction

This book constitutes another result of the cooperation between the Faculty of Law and Administration of the University of Lodz and Institute for Law and Informatics at the Faculty of Law from University of Lapland in Rovaniemi. This cooperation began in 2014 with the first international conference "Lawyers in the Media Society". With professors from Poland, Finland and Germany, Polish Inspector General for Personal Data Protection and Finnish Data Protection Ombudsman, practicing lawyers, doctors and doctoral students, this was a conference, which focused on exchanging knowledge and different approaches to some issues the lawyers face every day in the Network Society. It was not only a conference to conclude the NETSO research project (Network Society as a Paradigm for Legal and Societal Thinking) ended in December 2013, but first of all, a kind meeting between experts and practitioners in the field of ICT law and legal informatics from Poland and Finland.

With this book we hope to further explore the challenges of the Media Society as well as current issues related to the impact of information technology on the development of legal acts and regulations in the European Union with special emphasis on Polish and Finnish law. Papers, included in this book, focus on complex look at information technology within diverse research in the field of new technologies enabling the exchange of views and discussion from the perspective of legal doctrine and representatives of Poland and Finland. The papers are divided in this book into three parts: the first part presents the challenges of the information society, the second refers to the digital environment and the last includes texts, which explore the issues of intellectual property law and data protection.

We hope the book will be useful both to those less familiar with information technology, and those willing to further broaden their understanding of the changes in European Union and developments in Poland and Finland, which occur in the Media Society.

We thank all the authors for their efforts in presenting excellent texts, all the sponsors and Rector of the University of Lapland, Mauri Ylä-Kotola for making it possible to public this book.

Ahti Saarenpää, Karolina Sztobryn, Aleksander Wiatrowski

Part 1

Challenges of the Information Society

Chapter 1

LEGAL INFORMATICS TODAY – THE VIEW FROM THE UNIVERSITY OF LAPLAND

Ahti Saarenpää

Professor emeritus, Institute for Law and Informatics, Faculty of Law, University of Lapland, Docent, Faculty of law, University of Helsinki, Vice Chair, Finnish Data Protection Board, Finland, asaarenp@ulapland.fi

As one of the modern legal and communication sciences, *Legal Informatics* is very much a science concerned with different technological and societal changes. It has already been one for a long time. In fact, we should no longer speak of a new legal science; it is better to speak of a modern legal science.

First the computer, and then IT more generally, opened up new legal objects of scientific interest. They were both methodological, legislative and jurisprudential. Gradually they changed to become more essential objects of scientific inquiry. Indeed, in 1990 in a contribution to the Nordic Yearbook of Legal Informatics written with my teacher Professor *Aulis Aarnio*, I wrote that Legal Informatics is *an essential legal science* in the *Information Society*. I still have the same opinion.

That it was, and very much is so, although many representatives of the more traditional subjects wondered out aloud about the significance of the field. Lawyers are often conservative. It was no surprise then that Professor *Peter Blume* (Copenhagen) noted in his inaugural lecture at the beginning of 1990´s that *subject imperialism* in our university life had prevented us seeing the real value of Legal Informatics. That has very much been the case even later. More diplomatically, we could speak about the shadows which *tacit knowledge* often casts. We do what we have been doing earlier too. Not even the new Information Society was not enough to wake up traditional jurisprudence.

Today we no longer live in the *Information Society*. That era is already past. But it was a truly remarkable time, one when we began to use IT more or less as a tool. Office automation changed a lot in our daily work. The channels of communication changed. And the roles of information and information processing changed as well. There was good reason to speak of

the Information Society as a new society and, for example, to speak of "knowledge workers". One country after another sat up and took notice, drawing up a variety of information society strategies. The *European Union* was no stranger to this trend – not at all.

Today we may however arguably – actually we must – speak of a new *Network Society*. It is a society where our working and living environments typically depend on, and we are increasingly reliant on, information networks and on their proper function. The Network Society is also an *access society*. Disruptions in networks and software are no longer inconvenient glitches only. There are a lot of problems of quality with legal implications. And we should speak about the right to get access to open networks. It is already understood as a human right. Without access to open networks it is not any more to guarantee our *right to know*.

Like the Information Society*, e-government* is already an outdated concept. In the Network Society we should speak of *information government*. It is government that is dependent on the digital working environment. In the public sector, the smooth functioning of information systems is part and parcel of good government. Correspondingly, on the political level, we have witnessed a transition from information society strategies to *digital agendas*. A big change has taken place in our perspective.

Many legally important phenomena have now, quite naturally, made the transition to the network environment. All that is required is that we wake up to implications of the new environment. E-auctions are a good example. When Professor *Wolfgang Kilian* some ten years ago gave the first lectures in Lapland on e-auctions, we were in the thick of that transition. The new issue prompted interest and Legal Informatics was absolutely the right environment for discussing it.

Today, Finland's distraint authorities sell a considerable amount of the property they seize effectively using e-auctions. A more extensive change, one clearly associated with the Network Society, is reflected in the fact that where public procurements are concerned, Europe has now adopted tightly regulated e-auctions. In this case, we see that the era of traditional paper documents, as well as the legal life that revolved around them, are at least partly over. In Finland the legislative reform based on the Public Procurement Directive came into effect in October 2011.

The transition from the Information Society to the Network Society was not, however, merely a technological change and the additional regulation occasioned by such a change. What we see in addition are two other significant changes. Our *conception of the human being* has changed and the *rule of law* has become an ever more important way to structure the state.

These in turn are factors that have essential repercussions for the professional education required of lawyers. If these developments are not taken into consideration explicitly, what we may end up with are *narrowly trained* computer lawyers only. They would not shun the relationship between IT and law as such but they might lack relevant skills in two crucial respects: they would fail to recognize the depth of sources that inheres in human rights in the Network Society and fail to acknowledge the requirement – essential to the *European constitutional state* – that our fundamental rights be taken into account far earlier in the process of government and in fact all processes which in society are important from the legal point of view.

One relevant issue in the constitutional state in the new Network Society is *legal welfare*. This is a welfare that highlights human worth and, by extension, our right to self-determination. We endeavour to safeguard this welfare through the legal planning (design) of information systems and the receipt of information, as well as the legal quality of these processes. In keeping with this approach, our rights should as often as possible be realized as fully and as early as possible in any process. The path of information as a whole has become a crucial legal issue.

This is understandably an essential point of departure in our research and teaching in Legal Informatics in Lapland as well. It is a comprehensive perspective on the Network Society in the constitutional state, a view that is very much independent of the international very narrow, so called *proactive school* of thought.

At the same time as our rights have come to figure more prominently and ever earlier in legal, administrative and commercial processes, we have witnessed a marked change in the significance of *human* and *fundamental* rights in practical legal life. They have gone from being theoretical considerations to being tools used day in and day out in legal life. In interpreting the law, we can no longer content ourselves with domestic written law only as our source of law. Our interpretations must be situated in a context that is duly informed by *human* and *fundamental* rights. For many of those lawyers who have had traditional education and training in the field, this change in perspective has created and will create problems.

At the University of Lapland, Legal Informatics, like many other subjects, is divided into general and special components. The general component examines the impacts that the changes in IT and communications have had on society and citizens' rights and on the professional skills of lawyers. Thus everything mentioned above falls within the scope of general Legal Informatics. We do need that kind of general thinking.

The special component of Legal Informatics takes us to the level of more practical research and teaching. There we are accustomed to dividing Legal Informatics into four

different fields: *Legal Information*, *Legal Information Processing*, *Information Law* and *ICT Law*. We plan to continuing doing our research and teaching within this framework, although it's broad scope creates problems on the level of the individual researcher. We cannot expect anyone to master the level of detail required to be an *expert* in all four fields. But we should retain general knowledge in the component fields of Legal Informatics if we are to avoid the problems of the negative tunnel vision brought by specialization.

In fact, Legal Informatics has been very much *a methodological discipline*, a science that guides students to achieve appropriate and timely mastery of the big picture and that discusses the associated issues. Legal Informatics is still one of the general legal sciences and its general component is a significant field in itself, one that features interfaces with legal theory and the sociology of law. But specialization within the field is naturally essential in seeking the useful connection between theory and practice.

The *increased and continuing juridification* connected to IT seen in recent years has resulted in *Information Law* becoming slowly an area of law in its own right. The field, which at first confined itself to the protection of personal data, e-government and the regulation of traditional telecommunications, has expanded and continues to do so. It cannot go on without a program of legal research. In this research the role of information law principle is important.

Principles of information law are desperately needed in the new network society. Our systematics is almost blind without the idea of Information law. The deep going discussion about leading principles started during 90´s. Today, in a developed form, information law can safeguard our exercise of the right to self-determination and ensure the functionality of the information market.

The increased juridification will tend to bring experts from outside of Legal Informatics into the research arena too. Indeed, *communications law*, which we have taught for a good many years already at the University of Lapland, is an interesting and important forum for cooperation with researchers in communication. In this cooperation the role of information law principles is extremely important.

At the same time, the relationship between Information Law and the traditional Legal Informatics will change. In this regard, Professor *Maximilian Herberger* has pointed out to me that the change might well weaken the position of traditional Legal Informatics within the family of legal sciences. Here we without doubt see Legal Informatics facing a new challenge. The relation between theory and praxis does need more and more service all the time.

Legal information has long been one of the cornerstones of Legal Informatics in the Nordic countries. The contributions of *Jon Bing*, *Peter Blume* and *Peter Seipel* to research on

legal information management have been fundamental ones in constructing what became a *new Nordic legal information culture*. Nor has legal information management lost its timeliness. A sound knowledge of the fundamental of information retrieval and, more nowadays broadly, *information literacy* are very much part of any liberal arts education at the university level. They belong to our basic skills.

As a subject of research and teaching, legal information is a far broader field, however. It extends from our right to information – the right to know - and the availability of public information to the legal information management that forms part of the basic method of any lawyer used day in and day out. Leaving this subject-area wholly or primarily dependent on the expertise of other professions would entail a significant societal risk. Clearly, *Peter Wahlgren* was not wide of the mark in broaching the topic of *risk* in this connection. We do need cooperation between legal and information professions.

Alongside the different institutes of Legal Informatics we have seen – however primarily outside of Europe – the emergence of *institutes of legal information*. These play an important role in ensuring the accessibility of otherwise far-flung public-sector information. The EuroLII project, outlined originally by *Graham Greenleaf*, would continue these trends. The Institute for Legal Informatics at the University of Lapland is participating in the project, which is however still in its initial phases.

Earlier legal information processing as an elementary part of legal informatics was very much theoretical. Researchers were for example thinking about the question of whether a computer can replace a judge. Later has often been discussed about the possibility to build and use expert systems that support judges in their work. Today we are already witnessing the age, when *e-justice* is something practical.

We have progressed from the early technical development of office automation to the high quality required of the various implementations of e-justice in the modern European constitutional state in a sophisticated Network Society. Contrary to what many think, e-justice is not just one stage in the computerization of electronic administration. Rather, e-justice should be viewed as a significant step towards improving the quality of legal information, enhancing legal professional skills and promoting equitable administration of justice in the new Network Society. Appropriate e-justice services, appropriately implemented, further our right to information and to the equitable administration of justice in a constitutional state, a state that respects the rights of its citizens. We have taken a lot of steps from old theory to modern practice.

In speaking of Legal Informatics in Lapland, one cannot overlook the subject of *personal data protection*. Its development has figured prominently in the juridification of legal provisions in the area of Legal Informatics. The dimensions of data protection in the Network Society are utterly different than what they were in the earlier Information Society. At the University of Lapland, the teaching of personal data protection has in fact played a key role in the teaching of both *Information Law* and *Law of Personality*. This affinity continues, although personal data protection and privacy are separate fundamental rights in Europe today. In North American usage, they rather confusingly tend to be lumped together.

The Faculty of Law at the University of Lapland can justifiably be considered the Finnish centre of expertise on personal data protection. We also work closely with the office of the Data Protection Ombudsman. It is no accident that the Ombudsman, *Reijo Aarnio*, is an honorary doctor of the Faculty.

In speaking of personal data and the legislation enacted to protect those data, one must remember the importance of *information security* in the Network Society. After serving largely as a crucial factor in realizing personal data protection early on, information security has become an essential component of the constitutional state in the private as well as the public sector. If one plays by the book, one may not set up a business without comprehensive legal and technical planning or personal data protection and information security.

Back in 1997, the Institute for Legal Informatics of the University of Lapland drew up a report for the Finnish Ministry of Finance on the need for legislation in the area of information security. Our answer was positive. Unfortunately, the opinion of government was negative. The issue still figures prominently in our research and teaching in Legal Informatics. When EU is at last drafting a cybersecurity directive, we have a lot to do. As well for example the principle of *Open data* and the adding discussion about *neutrality of Internet* are challenging us by a new interesting way.

Legal Informatics is – and should be – one of the most international fields within law. That is why we are involved in not only the essential, inspiring Nordic cooperation but also in a range of international degree programs and research projects farther afield, for example, Chile. The research project *NETSO* – network society – is a good example of that. And our annual *International Summer School* is another means by which we pursue our goal of being international. Let me also mention *EULISP* LLM program and *LEFIS* cooperation. Scientific interoperability is to day extremely important.

Of late I have generally begun or ended my presentation with a reference to the United Nations Convention on the *Rights of Persons with Disabilities*. It is a significant human rights

agreement, adopted in December of 2006 and emphasizing equality among people. When it comes to our right to self-determination and support for that right we should be as equal as possible, with this equality encompassing *access* to and *opportunities to make the best use* of information networks. This poses a significant challenge for research and teaching in Legal Informatics too.

Chapter 2

KNOWLEDGE, INFORMATION, AND INDIVIDUALS

"Why waste time learning, when ignorance is instantaneous?"

(Calvin)

Wolfgang Mincke

Professor, University of Lapland

1. What is knowledge?

What is knowledge good for? Why is it necessary?

To know the way from town A to town B is good for not going a long way round and to save time and gasoline. To know poems by heart is good for boasting – and annoying other people. Knowledge apparently is good for solving cross words!

It must have been about this line that in the end of the sixties the idea gained ground that knowledge of facts was not as important as traditionally had been thought. Instead the focus should be on procedural knowledge, methodological knowledge.

This school of thought has been rather successful, perhaps not that much successful in furthering education but in discarding knowledge of facts: In school learning by heart was despised. No more capitals of states, no more year dates in history, no more poems by heart. There arises one question: What is a method or procedure about if you have no knowledge of facts, if you do not know the facts the procedure is to manage, what is the method or a skill to explain?

Without knowledge of facts you are fully committed to a method and bound to it. To make a choice between methods, you have to evaluate the findings, the results of competing methods. Which is the better among different methods? Apparently the one that better explains the facts, and the one that brings about reasonable results. Without knowledge of facts you cannot make this evaluation! This should be a severe warning of all ideologically founded concepts of education. This explains why typically regimes based on an ideology and which propagate this ideology firstly have to restrict the access to knowledge. It is the knowledge of facts that opens the possibility to think of alternatives. But what is a reasonable result? Or, in other words: What can we accept as knowledge? Or, what do we know? Socrates answered:

Nothing. I only know that I know nothing. This sounds like coquetry, but it has a good philosophical motivation. Popper has taught us that there are no assured truths, we can trust only in falsification. A more practical answer has the Finnish philosopher Niiniluoto: Knowledge is assured believes, assured, ascertained cognition. (*Tieto on hyvin perusteltu tosi uskomus*.)[1]

How does one assure believes, ascertain cognition, control the content of a statement?

- google it...
- look it up in Wikipedia...
- look it up in an encyclopedia....
- ask friends you believe to be cleverer than you are…
- ask an expert.

It is natural humbleness, when one believes others more than his own judgment - but this is not the self-contained, autonomous person we see as the goal of education and erudition and that we accept as a competent partner in argumentation, a person with an own judgment. How does such a self-contained, autonomous person evaluate what is reasonable?

Suppose: A friend has gone to Florence, in July. You get a message from him by E-Mail: Here it is terribly hot, 35°C! What to do with such a message? You will contrast it and check it with what you know. There are three main possibilities:

1. The message confirms what you already know.
2. The message tells you something new but is consistent with what you know.
3. The message contradicts what you know.

2. The informational interpretation

The three possibilities can be phrased in terms of informational content:

1. The message is not informative. Your knowledge remains as it was. You knew that Florence is in Italy; 35° is not unusual in Florence in July.

2. You might not have known where Florence is and what the weather there is like in summer. Now you know that much at least: It is pretty warm there in July. The message is informative, it adds something to your knowledge.

3. You might have thought Florence is a place far up North in Norway. Now you know: This can't be true. The third possibility is the most interesting case: the message says: There is something wrong with your knowledge. You have to change your world view. This is

[1] N. Ilkka, Informaatio, *Tieto ja Yhteiskunta (Information, Knowledge, and Society)*, Helsinki 1989, p.57.

the maximum information you can get from message. Such a message gives reason to become sceptic: Is it true at all?

Here we encounter something interesting: When we speak about “no information” (and that is minimum information) and maximum information - apparently there is something like an amount of information, a quantity that will vary in the cases between the extremes, at least in the sense of less and more information.

Apparently, information – in the sense “what is informative” - depends not so much on the message itself but mainly on the previous knowledge of the receiver of a message, on his expectations:

For an ignorant - a person who knows very little or nothing - everything is informative.

For average people like us what is informative depends on what we know, on our world view, on our expectation. For an all knowing person, an omniscient (if such a person exists) nothing is informative.

The ignorant is not very interesting, nor is the omniscient. We are interested in people like us, who have a world view, some knowledge about the world. We know where Florence is and have an idea, a certain expectation what the weather is like in summer in Florence.

But: The information the receiver gets from a message does not only depend on his knowledge but to a high degree on his competence to evaluate the information of the message: And this competence depends on his knowledge and on his capability to process the message, to track the effects of a message in his knowledge.

In the silly example of weather in Florence in July again: Imagine the message is not “it is terribly hot here” but: Last night here fell snow!

The ignorant might conclude that Florence must be somewhere near the North Pole or deep down in South America. And he might think: “Aha, weather is much better here!” The best he will get from the message would be a wrong world view.

An average person, who has an idea where Florence is and what weather can be expected in July, would think: That is sensational. I would never have thought that. That is impossible! And he would now imagine how traffic breaks down in the town and other consequences of snowfall.

Now think of a meteorologist. He has not only factual knowledge about weather in Florence, but he knows why it is hot in July in Florence. Snow in July is not only very unexpected, a sensation, but it contradicts his knowledge. He knows that weather in the seasons has to do with the inclination of the earth axis and would consider, whether something might have happened to this inclination.

It is apparent that an average person gets more information from the message than an ignorant and that the expert gets more information than the average person. With a conventional opinion one would think that the information of a message has to do with expectations, with the probability of the message. This is and remains true. But this does not fully explain the difference between the meteorologist and the layman in weather science. For both, when asked, the probability of snow in July in Florence would be zero, it is impossible in the world as they know it.

But apparently the message has more significance for the meteorologist than for meteorological layman. We could conclude: The amount of information does not only depend on the probability of an event, on our expectations. The more somebody already knows and the better his ability is to reason and his logical ability (this is the capability to track the consequences of a message in a world view), the more information he can get from a message.

3. Quantification

This more or less information means apparently that different persons get different amounts of information from a message. And this brings us to the problem, how to determine the amount of information.

If the amount of information a person gets from a message is mainly not in the message itself but depends on his previous knowledge and on his logical competence, it seems futile to look for an amount of information that could be determined objectively. Knowledge differs from person to person.

But an objective amount of information is just, what Rudolf Carnap and Yehoshua Bar-Hillel, two philosophers, where after in an article they published in 1952[2]. In this article they explored a measure of information. Their starting point was not real human knowledge and their logic was very simple: They took a very simple model consisting of three individuals and two properties. These made up their whole universe (our knowledge) to test a measure of quantification of information. If you want a more concrete situation: imagine an astronomer interested in three planets of a foreign star (the three individuals). And he is eager to get information whether there is water on them and whether there is life (the two properties). His "universe" (in this scientific project) is closed to these states of the planets under review.

How many answers can he get? There are 64 possible answers: none, one, two or all three of the planets have water or life or both, thus from none of them has water (w) or life (l) - to all

[2] R. Carnap, Y. Bar-Hillel, *An outline of the theory of Semantic information*. Research Laboratory of Electronic, Massachusetts Institute of Technology, Report No. 247, 1952.

of them have water and life. This is a combinatorial calculation with the formula $(2^2)^3 = 2^6=64$. Or, to be more elaborate: There are 4 possibilities for C (w+l, w-l, -w+l, -w-l). The same 4 possibilities exist for B, so we get 4 * 4, and again for A exist the same 4 possibilities, making 4*4*4 = 64 possibilities.

Carnap/Bar Hillel concluded: The maximum information one can get in such a universe is, when the two properties are determined for all three individuals (when our astronomer knows of all three planets whether there is or is not water or life). There remains a single possibility and 63 possibilities are excluded, and this is the maximum information our astronomer can sensibly hope for. The more possibilities are excluded – the more information you get. And this can be calculated and thus quantified in such a simple model. When the astronomer gets to know there is water on planet A, 32 possibilities are excluded. If additionally he gets to know that there is life on planet B, then 48 possibilities are excluded. Generally: The more possibilities are excluded the bigger is the informational content of the message - or: The amount of information is equal to the amount of excluded possibilities.

Of course, the model Carnap and Bar Hillel have used is far from realistic. They assume a receiver who has complete knowledge and perfect logical skill. For real life situations it is absurdly small (or it may fit for exceptional situations astronomers might be in). In real life we have to do with an indefinite if not infinite number of individuals (where "individual" means not only persons but everything that qualifies for an item to make statements about) and a number alike of properties such items may have. One could begin to doubt, whether it is sensible at all to ponder over the amount of information of messages.

But, of course, we speak about information of messages and sentences of all kind. And we do this very sensibly. Indeed, we do not try to quantify such information, but we compare the informational content of messages, as we have done here, and we state that it is very well possible to speak about more or less information. How is this possible?

We know the answer already: Our situation is not the one, Carnap and Bar Hillel have taken as basis for their analysis. When evaluating the information of a message we do not start from scratch, with no previous knowledge, where everything is possible with the same grade of probability. This led into the problem of immense numbers.

On the contrary: We have a world view. And this world view is a very, very small cutout of these zillions of possibilities. This world view, our own "universe", can be understood as decisions made among the immense number of possibilities. And these decisions are made possible by our knowledge of facts, which we accept as well founded, or by our assured believes, as Niiniluoto says, and which make up our knowledge. We have established ideas

how properties are distributed among things and persons. These are the basis of what we expect and what surprises us as new and informative. The universe has shrunk to something manageable, though it may be very large still.

A very important difference between the universe, Carnap and Bar-Hillel have taken as basis in their study and the real universe, we live in, is that their universe is complete, closed. All possible states are known. This was a condition for quantification. Such exact quantification is not possible in an open system. Our universe, our world view is open. We are conscious thereof that we never have complete knowledge of the world. We have to accommodate our knowledge permanently learning new facts enlarging our knowledge or correcting our beliefs, changing our universe. This makes exact quantification of the informational content of any incoming message impossible.

What remains of Carnap and Bar-Hillel's project of quantification of information is the possibility of a rough estimation, an estimation of the informational value of an incoming message. But even such a rough estimation will often be sufficient to compare the informational content of different messages.

And what we still can accept is that a measure of information is the amount of excluded possibilities by a message. The more a message restricts what we have thought to be possible, the more it contradicts our previous knowledge, the more of our previous knowledge a message suggests to be wrong, the larger is its informational content. In an open system, of course, we cannot restrict information to excluded possibilities. We have to take into account messages that do not contradict our knowledge but just enlarge it. Here the question of quantification gets a new turn. Following the model of Carnap and Bar-Hillel one could now think of a list of possible additions to our knowledge, but we have seen that in the real world this leads to unmanageable numbers at least, if the idea is not mad from the outset. Again we will be limited to rough estimations of the amount of information of a message, at most.

4. Logic and Information

Something very important that has to be explained for the property “informative” or simply to the property “new”: We refer to something as new and informative, if we have not known it before, when we have not had it in our consciousness. This is enough for communication in everyday life. But there are generally two different kinds of “newness”, which are not distinguished in everyday life:

Something may be new, because it adds something hitherto really foreign to our knowledge. It adds something to our knowledge and we have to check whether our knowledge

thereby only has been enriched, or whether it contradicts our previous knowledge so that we have to correct it.

The other way something is new to us, is when it is only subjectively new for us, though it could have been concluded from the knowledge we already had. It is only new to us, because we did not realize this as a consequence from what we already knew. This is what Kant calls analytic judgments:

...a great, perhaps the greatest, part of the business of our reason consists in analysis of the concepts which we already have of objects. This analysis supplies us with a considerable body of knowledge, which, while nothing but explanation or elucidation of what has already been thought in our concepts, though in a confused manner, is yet prized as being, at least as regards its form, new insight. But so far as the matter or content is concerned, there has been no extension of our previously possessed concepts, but only an analysis of them.[3]

The same idea can be found with Descartes:

But, on examination, I found that, as for logic, its syllogisms and the majority of its other precepts are of avail rather in the communication of what we already know, …. than in the investigation of the unknown.[4]

Or in plain words: Logic is good in explaining what one already knows or could have known, it does not help to learn anything new that cannot be inferred from previous knowledge. But it says something about knowledge: that a distinction has to be made between inferable knowledge and really new knowledge.

Kant and Descartes do not speak in terms of information. But they can be interpreted informationally: Everything that can be deduced logically from existing knowledge (or any analytic judgment as Kant would say) seems only to be informative because it removes subjective ignorance or doubts. Objectively such inferable knowledge is not informative; the facts where from to infer have been known and the rules of logic have been known.

To sum up: The basis of information as understanding what happens in the world are knowledge and the ability to process this knowledge, thus: logic. The ideal would be a person with complete knowledge and perfect logical skill. These are the conditions Carnap and Bar-

---

[3] I. Kant's Critique of Pure Reason, Translated by N.K. Smith, London 1929, p. 47; Kritik der reinen Vernunft, p. 51: *Ein großer Theil und vielleicht der größte von dem Geschäfte unserer Vernunft besteht in Zergliederungen der Begriffe, die wir schon von Gegenständen haben. Dieses liefert uns eine Menge von Erkenntnissen, die, ob sie gleich nicht weiter als Aufklärungen oder Erläuterungen desjenigen sind, was in unseren Begriffen (wiewohl noch auf verworrene Art) schon gedacht worden, doch wenigstens der Form nach neuen Einsichten gleich geschätzt werden, wiewohl sie der Materie oder dem Inhalte nach die Begriffe, die wir haben nicht erweitern, sondern nur auseinander setzen.*

[4] …Discourse on the Method of Rightly Conducting One's Reason and of Seeking Truth, http://www.literature.org/authors/descartes-rene/reason-discourse/chapter-02.html…

Hillel have assumed in their model and this is what they have termed the "semantic information" of a message.

We have to live with imperfection in knowledge and logical skill. Both are given to individuals in varying degrees. This is the reason for perhaps the worst inequality in all societies, even worse than the inequality between rich and poor.

5. Societal importance of information

Since long time society has reacted to inequality of knowledge: schooling, even compulsory schooling, from kindergarten to post-doctoral studies. There is no doubt that the acquisition of knowledge can be furthered. It might be questioned whether logical skill can be taught to the same extent – though it is surely possible up to a certain degree. (One might have a suspicion here that teaching methods is just a substitute for teaching logical skill, though methods can be seen as selection and predetermination of logical possibilities.)

If our world view depends on knowledge and logical skill, and if it is mainly knowledge that can effectively be furthered in society, it is a consequence that access to knowledge is the main means to diminish inequality and further equality in society.

Knowledge is not only good for erudition. Knowledge is the basis of all decisions we make. This is commonplace in economics, where better information offers better chances. Economists could even be seen as pioneers of equality of knowledge, when economic theory classically has assumed consumers as perfectly informed persons, and in a special case, when it is striven to preserve equality by sanctioning the use of insider information. But knowledge plays a main role in all spheres of human life. Knowledge is the basis of an authentic world view. And nobody should be excluded from an authentic world view.

Access to knowledge is so important that one might wonder that it has not got an own article in constitutions. Mostly the access to knowledge and information is derived from the regulation of freedom of expression, the argumentation here above could suggest to find the core of it already in the principle of equality. The clearest wording can be found in the European Convention on Human Rights, where the second sentence of art.10 para. 1 reads: "This right (sc.: to freedom of expression) shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."

Indeed, when one begins to think about it, a right to knowledge seems unruly as a concept. Could a right to knowledge mean that you have a right to know everything that is known somewhere in the world? Or that you are under a duty to make public everything you know, because of the right of others? Neither seems sensible. Though, there might be an ethical

obligation: Imagine somebody who has discovered a cure against a certain disease. Isn't he under a moral duty to make this knowledge known to the public? Or, are scientists obliged to make known all their insights - at least when they hold an office?

Indeed, on the European level a right of access to information has been awarded by the Directive on Environmental Information[5], by the Regulation on Access to Documents[6] and various freedom of information legislation in different countries. This legislation is important enough, though it is limited in its scope to documents and information held by public authorities. This is much too narrow.

More important perhaps for general knowledge is information not held by public authorities, but general information public authorities aim to influence or to suppress. There is no need to tell examples, history is full of them. We are permanently witnessing still suppression of information in a lot of states. This suppression is not only an assault upon a specific right; it is an assault upon the personality as a whole: It should have become clear that everybody has the right to develop an authentic view of the world and this presupposes access to all available information. There arise questions beyond the known problems of protection of personal data and problems of public security. With another facet of the problem one could ask, whether it is admissible to let media influence people with questionable information.

But who is to decide what is authentic? Many would like to take that position, we should beware of them. The best we can arrive at is an attitude that is open for competition of opinions and leaving the decision which to follow to us. As a rule one could state that nobody may interfere with our cognitive abilities. This would be not more than a generalization of the formulation the Convention on Human Rights has used in its art. 10. The concept of semantic information does not contribute much to the formulation of such a rule. But it helps to see and underlines the importance of such a rule.

Though the concept of semantic information is important enough as a means for the understanding of an elementary condition of human life, its importance is by far not exhausted thereby. Some examples might illustrate that.

6. Meaning of sentences

What is the meaning of a sentence? This question seems trivial, but it is not. There is a lot of discussion about the meaning of words and concepts. Since the Middle Ages nominalists, conceptualists, and realists have disputed about the meaning of concepts. In modern times we

[5] Directive 2003/4/EC.
[6] Regulation 1049/2001.

have heard about the difference of extension and intension of a word, with the widely known example of morning star and evening star having the same extension, the planet Venus, but different intension. Much less popular is the discussion about the meaning of sentences, of statements, though there is a proliferate abundance of theories.[7] Semantic information can perhaps give a relative simple clue to approach the problem.

We will use in a very loose manner the model of a universe as Carnap and Bar-Hillel have proposed it, where propositions have to be tested against a universe of possibilities. Thereby one might get a rather simple answer to the question, what a sentence means. We imagine our own individual knowledge as the universe, where the meaning of a sentence is considered. The sentence will have a certain significance by being in accord or consistent with what we know and excluding other possibilities as inconsistent with the statement. One might be tempted to see the meaning of the sentence as pointing to or as a reference to the whole bulk of consistent possibilities in our knowledge, but that would not be very illuminative. Especially, as an everyday experience, we know that we ourselves do not immediately oversee all our consistent knowledge (and in this "knowledge" might even hide inconsistencies).

A better proposal than to look at the consistent possibilities as the denotation of a statement perhaps would be to understand the meaning of a sentence as an instruction to draw the line between possibilities consistent with the statement and excluded possibilities. It might be simple to draw that line in a systematically ordered knowledge like the universe Carnap/Bar-Hillel use. In our chaotic knowledge the division into possible and excluded possibilities cannot be designated by a line. This character as an instruction explains, why the meaning of a statement does not have to be instantaneously clear. It may take time to consider its effects in one's universe.

It is a consequence of this model of meaning that meaning has a subjective background. The individual universe decides what is in accord with one's knowledge and thus subjectively true. This explains why "snow in Florence" may have a very different meaning for different individuals, depending on their previous knowledge or expertise. On the other hand this difference should not be exaggerated. One can take for granted that to the greatest extent our knowledge is homogeneous, shaped by homogeneous everyday experience. It is this homogeneity that makes communication possible. This might vary in different cultures and different environments. We can assume that in comparison with this homogeneous knowledge

[7] Cf. Wikipedia s.v. Meaning (philosophy of language).

it is a very small layer on top of it where knowledge is formed by individual experience or expertise.

7. Understanding

It is a very short step from meaning to understanding. What does it mean, that somebody understands a message? In ordinary talk this seems unproblematic. Somebody has the intention to present something he has in mind, and if the receiver can reproduce this in his mind, he understands the message. But, one should doubt that this is ever exactly possible.

Understanding can be described as grasping the meaning of a statement, the process of unravelling its information. Meaning can be looked at as something objective. A statement has a meaning, whether the work of testing it for consistency with individual knowledge has been done or not. Above it has already been pointed thereto that we are not instantaneously conscious of our whole knowledge even ourselves, we do not have a place outside ourselves to get our knowledge before us and to look at it. This makes understanding subjective, individual. And here not only the individuality of knowledge decides but the second element comes into play, the skill to check a statement for information. This is the logical ability to see, whether the informational content of a message can be derived from previous knowledge, whether it extends this knowledge or whether it is in conflict with such knowledge. And this ability apparently varies from individual to individual.

Of course, there are everyday situations of understanding where we have an immediate understanding, when commonplace knowledge that can be presupposed from everybody is concerned. In such situations one can count thereon that a message is understood immediately. But even such texts may comprise surprises. But generally the process of understanding is not an instantaneous event, often it is a process where the content of a message with its consequences becomes conscious only successively and after long pondering. Everybody in science has had this experience.

It is a somehow very astonishing fact that texts that are thousand or more years old can be spoken about, revealing new insights and showing actuality. This can have to do with implications these texts have always had, but which are revealed only now. But a more usual reason is perhaps that our knowledge, our experience, our expectations have changed, changing or expanding the information of the text, giving such texts a new meaning and thereby demand a new understanding.

8. Music

We can loosen the model of semantic information even farther and speculate about phenomena that are not bound to language. Why do many people have difficulties with so-called modern classical music? The usual explanation is that we are accustomed to a certain kind of tonality, some even maintain that this is innate. Classical music is based on the tonic, the dominant, and the subdominant. In this setting we experience musical tension or friction and relief or possibly simple dullness, too. This musical setting can be seen as equivalent with a universe of knowledge, making up one's expectations. Without such a universe we have no expectation, we have no norm, no criteria, we do not know what to exclude. Shortly: Such music has no information for the conservative listener. This does not exclude that non-tonical music has an own setting, an own universe. We find different settings in Arabic music or in the pentatonic music of the Far East. Or compositors might invent own settings which – without explanation - can only be opened up from the composition itself. This explains perhaps why performing musicians seem to have a better access to modern music. They have to deal with their music much more intensive than pure consumers and may find a new order and information beyond harmonics.

9. Science

Above we have stated that it is impossible completely to render knowledge understood in real life; the immense number of possible states is an unsurmountable obstacle. Therefore, the information of a message will better be understood not as a confined picture of situations but as an instruction to delimit what is in accordance with the message and what is excluded by the message. In the outcome personal knowledge and logical skill will decide how much and what information somebody draws from the message. This is the case in normal life situations.

This is not enough in any field that thinks itself suitable for a scientific approach. What we expect from science is clear answers. Any science must create and uphold a view of its field that makes it possible to unravel the information of a proposition concerning its realm. And this view has to be intersubjective, not bound to a personal knowledge (though of course the command of this knowledge may greatly vary even among experts). This does not exclude that scientists have very own ideas and subjective judgments. But there has to be a level to discuss and to judge the value and qualification of deviating opinions.

The discussion which criteria a field must fulfill to get the status as a science has a long history. A first and necessary criterion seems to be the endeavour to find a means to make the information of assertions in a field of knowledge traceable (though it is perhaps not sufficient,

in the sense that every such endeavour in any field has to be seen as science). Then all sciences are informational sciences. This makes the difference between scientists and engineers.

To make the information of assertions traceable might begin simply by collecting and fixing the established knowledge of a field. This could start with an encyclopedic collection. A next step could be to bring this collection into some thematic order. But a developed science will have seen the need to ease the disclosure of information of propositions. An established means to facilitate this is the presentation of knowledge in a systematic manner. This does not only help to find relevant knowledge. A successful system will have a logical structure and thus facilitate to keep the knowledge consistent.

What we expect from any science is that it gives the possibility to evaluate whether a proposition is in accord with existing knowledge, whether it adds something new to existing knowledge or whether it contradicts it. The evaluation, whether the proposition under review is in accordance with existing knowledge, if done in a formally correct manner, is commonly named a proof. It is here where logic comes in: A proposition is proven to be scientifically valid if it can be derived logically from established, accepted sentences in that science. We all know this from mathematics in school, when for instance Pythagoras' theorem has been proven. The usual way is to deduce a proposition from more elementary accepted more general sentences.

On the contrary the failure of a logical proof might demonstrate, that a proposition contradicts generally accepted knowledge. Very often this indicates that the proposition under review is simply wrong. But it can signify, that parts of the hitherto accepted knowledge are to be abandoned. A famous example for this was the case in astronomy, when Copernicus found out that Earth circles around the Sun.

A third possibility is that the proposition neither can be proven, nor does it contradict existing knowledge, either. We exclude here overly speculative or nonsensical propositions. The possibility of a new insight is always given, because in all scientific systems we have to do with open systems that demand additions and completion. An impressive example of this was the formulation of the periodic system of elements by Mendeleev. This system did not change knowledge of the hitherto known elements, it brought them into an order and opened the door to further insights. Thereby even the existence of elements which were not known yet could be predicted.

To give this an informational interpretation and applying the basic cases of semantic information: If a proposition can be derived in the system, if it can be proven to be valid, the proposition does objectively not extend our knowledge. The sentences wherefrom the proposition was deduced were known, the rules of logic used in the deduction were known. So

the proposition tells nothing new. Only the deduction itself had been undone. Somebody with perfect knowledge and perfect logical skill would have known this before: So this sentence has no objective information.

If the sentence cannot be derived, because it tells something new, the knowledge base of a science is extended. This case did not arise in the model of Carnap/Bar-Hillel. Their knowledge base was closed, there was no new knowledge. But in an open system new, added knowledge has apparently information. This information is not only that an item is added to the knowledge base. Think of Mendeleev's periodic table again: It not only brings the elements into an order, it opens up insights into the nature of elements: their number of protons, their electron configuration, their chemical properties etc. It will not be clear at once, what the amount of information of such discoveries or inventions is. Often connections with other parts of the established knowledge will become apparent only gradually, by and by. In the end historians will argue over the importance of discoveries (and then they argue over the amount of their information).

If the sentence contradicts established knowledge (and the sentence is true), this can mean a revolution in science. At least parts of it are wrong. The established knowledge has to be revised. In the closed model of Carnap and Bar-Hillel a single contradiction makes the whole system worthless. Logicians can show that in a system with a contradiction any sentence can be proven to be true. So, Carnap and Bar-Hillel found in contradictions the maximum of possible information.

But we can still use their thesis that the amount of information of a proposition, sentence or message is the bigger, the more knowledge is excluded by that proposition. This seems to be counterintuitive for many, perhaps because one is inclined to find information in the meaning of the sentence as pointing or referring to something positive rather, than as pointing to excluded cases. But think of Kepler who found out that the planets do not go round the sun in a circular orbit but in an ellipsis. Whose discovery had more information? Though Kepler's discovery has opened the way to many new insights, I think that Copernicus' discovery had more information just by overturning a whole world view. Keplers discovery was a correction of Copernicus rather. And this seems to be the preferred opinion of historians, when they speak about the Copernican Revolution.

10. Legal Information

This all is of eminent importance for the science of jurisprudence. If it is the task of any science to render its established knowledge in a communicable and reproducible form law is an

exemplary model as a science. Since the days of Menes in Egypt or Hammurabi of Babylon it has been the endeavour of lawyers to render their material in an ordered form. Jurisprudence has come a long way from more or less ordered lists of rules to modern more or less systematic codifications.

From the outset all codifications can be seen as not only guiding jurisdiction but as delimiting arbitrariness as well. And so they continued to do up to the elaborate codifications of our days. In all developed legal systems lawyers are bound by their respective legal order; this holds for all professions employing law: judges, advocates, commercial lawyers, administrative lawyers, etc. And this is what we expect from their reasoning: that they show that their decision, pleading, advice is derived from valid law.

In this function as a confirmation that a decision is consistent with the valid legal order legal reasoning corresponds to or even equates to proofs in other professions. However one arrived at a result, this result preliminary has to be seen as a hypothesis that has to be tested for consistency with the established rules of the respective science. Ideally the justification of a decision has to demonstrate that it was arrived at without change or modification of existing rules or invention of new rules. In a sense this means that the result has no information. Of course, the result and the reasoning behind it might be (subjectively) informative for somebody because actually he has not verified this reasoning himself or because he was not able to do so. But for a legal expert with perfect knowledge of the legal order and perfect logical skill the result would have been clear from the outset: for him the result says nothing new, it has no information. The decision renders just what the legal order contains for this case.

It is perfectly clear that such unambiguous results are by far not always to be expected, such results even might be seen as exceptions. Such cases have been termed figuratively as “soft cases”. What keeps lawyers busy are so-called “hard cases”, where a clear-cut result does not show up unambiguously. The reasons for this are manifold: Difficulties begin with subsumption. The law uses categorizing concepts: the facts of a case must be brought under such categories. But, whether an item belongs to one category or another or whether it will demand a new category cannot be decided by logic. It is mostly common sense that leads subsumption and there is usually broad room for disagreement.

This is where interpretation comes in. Surely, for advocates and other practicing lawyers there will always be the tendency to steer interpretation of a rule into a direction that serves best the aim he has in mind. He will see that his interpretation supports the claim of his client or his superior. Then usually there will clash two interpretations of two representatives of two disagreeing parties.

Things become even worse, when a rule does not only offer room for interpretation but when it becomes apparent that there is no rule for the problem in question, when the legal order seems to be incomplete, when there is a lacuna in the law. Lawyers will argue similarly as in interpretation to fill in the lacuna.

What characterizes all hard cases is that lawyers not only apply law but they work on the legal order, clarifying, modifying, completing it. Now, undeniably what they do has informational value, it maintains something clarifying, modifying or completing the legal order, something new that is not – yet - established legal knowledge. This same holds for judges interpreting or completing the law in their decisions. Legislation is by definition informative (if it is not only reformulating existing law).

Legal science has traditionally offered tools for the situation that a clear rule is missing: For interpretation different methods are offered: grammatical interpretation, historical interpretation, systematic interpretation, teleological interpretation, etc. For situations of lack of an appropriate rule: Try to find a norm top down from an established rule, *a maiore ad minus*, or try it bottom up, *a minore ad maius*, or find somewhere a regulation that is comparable and apply the idea of this rule analogously, or argue that any other interpretation would lead to absurd results. Further, law has stated general principles, governing legal regulations: that contractual parties have to act in good faith, that goods are transferable, that rights can only relate to specific goods, and many more.

Such rules might seem useful but they have a crucial flaw: There is no "meta-rule", when to use which method of interpretation, the rules of interpretation defy logical treatment. But this should be no more a surprise after what has been set out above about the relation between logic and information: Objective information begins where logic ends, informative in the objective sense is only what cannot be deduced logically.

What are these rules of interpretation then good for, what is their sense? For an answer one has to start from the outset again that lawyers are generally bound to the established legal order. Informationally this can be understood as a command that they have to avoid inroads into the established order or that they have to minimize information, understood objectively as changes of existing law. Even if the law is not clear or if the law needs completion, this does not give lawyers arbitrary power to emend or complete the law. They have to find a solution that is as near as possible to existing law. In this task the rules of interpretation give advice: Try an argumentation top down from an established rule, or try it bottom up from another rule, or find a comparable regulation and look by which method you arrive at a solution for your case that minimizes the inroad into existing law and keep care that your proposal does not conflict

with general principles of the legal order. And this means: Keep the information of your solution as low as possible.

This sounds very conservative and indeed it is this far - but it has not necessarily to be. Clearly it might make law unattractive for revolutionists or demolitionists, but it does not hinder development and progress in law. Rules of interpretation, general principles are not categorical commands, they can be understood as standards indicating where specific argumentation is required. What we may demand from any argumentation that goes beyond established law is that it either shows that it only adjusts the existing law or indicates and justifies where it modifies or even overrules established law. This means that any decision owes us its informational content.

Chapter 3

LAW: LINEAR TEXTS OR VISUAL EXPERIENCES? CHALLENGES FOR TEACHING LAW IN THE NETWORK SOCIETY

Ahti Saarenpää

Professor emeritus, Institute for Law and Informatics, Faculty of Law, University of Lapland, Docent, Faculty of law, University of Helsinki, Vice Chair, Finnish Data Protection Board, Finland, asaarenp@ulapland.fi

1. Since the invention of writing, the history of legal information has largely been a history of texts. In most countries these texts have been linear. Laws, cases and the legal literature are mostly presented in the form of text. We consider this natural, and in fact essential. In a word, law, judgments and professional literature are written. How they are written of course varies from country to country depending on the particular legal culture.

2. Correspondingly, laws are read. Reading is one of the cornerstones of legal life. In somewhat simple terms, legal interpretations are – and should be – based principally on what written legal sources tell us. In the Finnish legal literature, I have described lawyers as 'text eaters'. We are really reading law. And a good lawyer is a genuine document management professional.

3. This mastery cannot be gained by picking and choosing what one reads; such an approach has never worked. Indeed, in his study of Swedish lawyers' working routines in the early 2000s, Professor *Claes Sandgren* concluded unequivocally that spacious and well-stocked bookshelves improved the quality of lawyers' work. And this is what books do, provided we really use them. Traditional legal literacy is one cornerstone of quality in our profession.

4. A remarkable step forward was taken where books and their bibliographical organization were concerned when we made the transition into the age of databases and, from there, to using more extensive electronic information stores. Above all, professors *Jon Bing* in Norway and *Peter Seipel* in Sweden demonstrated for the Nordic countries that the professional skills of a lawyer – a good lawyer – had come to include a new component: information retrieval skills. This observation meant that the basic method of the lawyer had taken on an additional

element.

5. *Seipel's* famous statement that sloppy information retrieval can make you 'lose your case and lose your face' rather says it all. As a member of the Disciplinary Board of the Finnish Bar Association, I have certainly run into my share of such cases. Lawyers are required as part of their professional skill to have a profound knowledge of the bodies of legal information. This is naturally also an aspect of good advocacy.

6. Today we live in the new Network Society. We do our work on information networks and using information systems; we are highly dependent on them and the information they contain. Information retrieval skills have become more important than ever. In fact, one hears the term 'information literacy' being bandied about quite commonly. One essential component of that literacy is the ability to read legal information in digital environments.

7. This skill has meant another important enhancement to professional skills. Familiarity with individual legal databases and their information retrieval procedures is not enough in our legal life today. Then again, narrow specialization is also a significant risk: it easily results in one having scanty information – and, eventually, scanty skills to match – when it comes time to deal with new questions or old in the new legal framework.

8. One tried and true remedy is often better than a bag of new ones. Indeed, it is very much still the case that extensive bodies of information, a uniform query language for them and free-text searches are indispensable aids in information retrieval. The stores of legal information compiled and made available by legal information institutes (LII), adhering to these principles as they do, have become crucial information products in some countries. This can be considered a significant part of the development of modern legal culture. We see the academic community acting as a producer of information.

9. An example of such a product – albeit on a smaller scale than seen elsewhere - is the Finnish database Edilex, produced by the state-owned company *Edita*. Edilex makes all Finnish legal journals available to the legal community through what is known as the Law Library. The resource also contains a significant amount of other materials, for example, the literature published by the company in electronic format, articles that have appeared in electronic form only and an extensive selection of master theses. However, Edilex is a commercial legal information service, not a national information store in the proper sense.

10. That function is in Finland partly served by Finlex, which is an extensive database of official legal materials hosted by the Ministry of Justice. It is limited to official materials and as such fulfils government's basic obligation to make legal materials available to the public. The resources *Lagrummet* in Sweden and *Lovdata* in Norway reflects largely similar

approaches.

11. In technological terms, one advance has undoubtedly been the development of mark-up languages. In a digital environment, it becomes essential to consider how data is attached to an IT platform.

12. Legal XML and other corresponding languages offer opportunities for increasingly flexible access to documents in different information stores. Document logistics and document workflow are crucial considerations where information maintenance is concerned. In the constitutional state we must consider the entire path that information travels, paying due attention to technical solutions as well as content. And every lawyer out there in the work-a-day world should realize their significance; this should have been driven home as part of their basic training. Professors *Monica Palmirani* (Italy) and *Cecilia Magnusson-Sjöberg* (Sweden) have done a great deal of important work in this area.

13. Thus far I have been talking about texts and how they are presented and read. This has been an essential point of departure given that the topic is legal information – information that is created primarily in the course of usual textual communication. This is not enough, however. As we know, different kinds of legal images and signs also have a rather long and multifaceted history. Let me bring those into our discussion too.

14. The most typical legal signs today are the *copyright symbol* and *traffic signs*. To be sure, the former has almost totally lost its significance - at least in Europe - but the latter have become increasingly important. In our increasingly complex world, a traffic sign is a solution designed for situations where text would be too slow a medium. Law, too, would benefit if it could draw on multiple senses through the use of written, visual and oral sources, that is, texts and signs and voice.

15. Traffic signs are also regulated internationally, a telling reflection of our increasingly international world. The information on what is right and what is wrong in road traffic is everyone's business. As well, the signs should be simple enough.

16. Information networks have been described as information superhighways. This traditional and apt expression rather compels us to consider the need for traffic signs on such highways – as an addition to the copyright sign and privacy clauses already required by law. But where are the traffic signs on the Internet and other networks?

17. The new EU Data Protection Regulation will provide guidance on the standardised use of data protection signs and seals. This is an aspect of improving openness and reliability in the processing of personal data. The aim here has been to move forward from case-by-case consideration – manual labour of sorts - towards an era of standards. The credibility of

content will be indicated using standardised signs. In a sense, these are traffic signs on the information superhighway. Given the importance of personal data protection, I consider this step forward taken by the EU Commission to be a significant one indeed.

18. Yet the visuality of the law is a far broader issue than the more active use of legal signs and images connected to legislation. In broaching the issue, we must ask in a new way: What does the law look like?

19. This question must not be confined to procedure, to the matter of a fair trial. Its scope must be broadened to encompass what legal texts and documents look like in the Network Society and, in particular, what the law looks like on information networks and information systems. And of course we should also remember traditional legal images and even law court architecture. To my knowledge, maintaining the dignified appearance of law throughout society is still an important matter.

20. Everything has its beginning and its time. Thus, legal images and signs have spectacularly long and varied histories in different legal cultures. The illustrated legal texts of the Middle Ages are a superb example of this. Here I should point out that Finland is one of those rare countries where judges nowadays do not wear a particular court uniform and where there is no particular courthouse architecture. Most law courts are located in state office buildings along with other government offices. Our administration of justice is visually impoverished. Unfortunately.

21. Research on the visual dimension of law has picked up in recent years. We remember well what Professor *Ethan Katsh* in USA has written on the subject on many occasions. It was he who in fact opened up the modern discussion of law in the digital environment.

22. And Doctor *Colette Brunschwig* of Switzerland has been a central figure in the field in Europe. She has especially written about the need for a new, multisensory law. The visual dimension of law has also been a staple section at the annual IRIS conferences in Legal Informatics. There, too, Doctor *Brunschwig* has been a prominent contributor.

23. And of course we should not forget the strong research tradition of legal semiotics. As the study of signs and meanings, semiotics has necessarily attracted the interest of legal scholars. Then again, the core of semiotic research is still focused primarily on texts and their background.

24. Equally salient and noteworthy in this connection is the significant work done by Professor *Zenon Bankowski* and more generally the "Beyond Text" tradition in critical legal scholarship. Professor Bankowski has sought in an engaging way to expand his interest in texts

to include the visuality and even art associated with them**.**

25. The visuality of law is, as we could see, not exactly a novel topic. We should always keep this in mind when discussing about new trends. Rarely, if ever, is something new – or advertised as such – wholly new. This is an essential point of departure in academic work, and one that we have to adopt when working in Legal Informatics, which is often billed as a new field. Any search for the scientific truth requires a sound knowledge of the research that has been done in the field**.**

26. I would now like to go on to take a look at some of the potential that the visuality of law might have in teaching law; of particular interest to me here are the development of legislation and e-justice. What follows is certainly not meant to be an exhaustive treatment of the subject. What I hope to do is open up one more discussion on the topic.

27. At its simplest, making law more visual has been seen as a matter of using some simple images – or, trivially, even individual lines – to draw attention to particular content in legal communication. One can also see the use of different cartoon-like drawings.

28. In this connection I will not have anything to say about these efforts, in either a positive or negative vein. My interest lies in how, in this era of the Network Society and constitutional state, the text of the written law can or, rather, should, be made more visual and in a way that enhances its legal value. I would also like to take up certain situation where visual law could be used in the digital environment. What is at issue here is more than the use of visual enhancements in conventional linear texts in traditional document environments.

29. I should start by distinguishing at least four different important perspectives: those of the citizen, the public official, the lawyer and the student. We should avoid oversimplifying the issue. And we must always remain mindful of technological developments.

30. Laws are – or at least should be – made for citizens; they are not designed particularly for lawyers or public officials. And as texts they are in principle the same for everyone. The reading skills of the users, however, differ profoundly. With this in mind, the Finnish government has, among other things, recently published a version of its democracy policy report on open and equal participation in Plain Finnish. However, in our legal profession there is, unfortunately, a tradition of thinking that legal texts are difficult to understand and are thus mostly the province of trained lawyers.

31. When we think of citizens' traditional obligation to be familiar with the law, the various programmes designed to improve regulation – like the EU's better regulation programme - have always included clarity of legislation as one of their essential goals. In a modern citizen-centred democracy, legislation should be simple. But achieving this simplicity

using written text alone is most likely an unattainable goal. Texts almost always open up a range of potential interpretations, for laypersons as well as professionals. This is one of the reasons why we need lawyers in society.

32. Of course we can improve drafting techniques to try to improve the clarity of the law. The preambles and definitions of concepts we see in EU directives and regulations offer one model for how to do this. But this approach quickly ignores the perspective of the ordinary citizen. The draft EU Data Protection Regulation (COM (2012) 11 final) is a striking example of this: the text of the instrument, which is supposed to be clear, requires a wider body of text – recitals - before it can be understood properly.

33. A better-functioning solution is for the text of a law to provide a brief, clear description of the relevant legal principles. At least some legislation can be officially drafted and adopted such that the text of the law gives a brief description of the human and fundamental rights on which the instrument is based. In this way the reader can be made better aware of the *deep structure* of the legislation.

34. Yes, the deep structure of law. In today's constitutional state we more clearly than before find ourselves in a situation where the direct application of human and fundamental rights is one of the threshold questions in our legal decision-making. The rights must be applied if a piece of legislation as such does not provide enough support for a particular legal or administrative decision.

35. Given the path that legal information takes in Europe, this requirement points to a substantial gap in legal certainty where language is concerned. To date, the judgments of the European Court of Human Rights have been generally handed down in English and French only. Fortunately, the European Court of Justice has already progressed to an effective multilingual policy.

36. The increasingly mandatory nature of human and fundamental rights in legal life undoubtedly prompts us to recall the norm pyramid of late Professor *Hans Kelsen*. The triangle as such was not, as the leading Kelsen scholar of our time, Professor *Oscar Sarlo*, notes, terribly important to Kelsen. More significant was the structured nature of norms.

37. Today this structure is easy to illustrate on a computer screen using various multidimensional shapes and, for example, coloured elements. Here we clearly have an interesting challenge for the new type of multisensory and written legislation. We can create new, effective legal signs – even 3D signs - and new ways of presenting legislation in addition to mere linear text.

38. For this we need the new traffic signs of the constitutional state. And not only

static traffic signs. The digital environment can free us from the shackles of the static text display. The structural elements of a legal text can be made visible to the reader in a mobile, dynamic form. Legislation, like other legal texts, can be given a visual identity.

39. I have myself spoken before on various occasions of "interactive legislation". By this I mean legislation which offers background information in the same information space for those interested in such information. Interactivity in this context in technical terms would mean above all that the information space would actively offer the user supplementary information. Written law could be a visual experience too.

40. We would no longer have to be reliant on static links and static texts. If we add to this accepted signs of the law, what we create from the average citizen's point of view is novel, partially visual legislation. It could wake up us to the deep structure of law. This change would naturally require that we also change the very meaning of 'legislation' as a collection of written law only. It should be something more.

41. We face a somewhat different situation when we examine the legislative environment in which public officials work. Regrettably often – at least in Finland and other Nordic countries – this consists largely of various sets of guidelines. Moreover, most government officials have no legal training. In a certain sense, administrative staff become paralegals to a considerable extent. This gives rise to – and should – particular demands regarding the legal source materials such staff use. They need something above and beyond the text of the law proper, something that is acceptable in terms of the sources of law. One important question is – and has been for a long time - the influence of precedents. Finland is not a country where precedents are binding. How can this be shown officially when managing precedents? At practical level code of conducts can be effective tools in this connection. However, they do not belong to our official legal sources; not yet!

42. In this connection we cannot overlook the international developments in e-justice. We are entering an era in which the traditional work of the courts and administrative officials - like everything else we do - increasingly takes place in a digital environment. This changes the informational environment in which decision makers operate. Their work has become dependent on information systems and networks.

43. In Finland we are currently planning two special workstations for judges. One is for those working in the general courts (AIPA) and the other for those in administrative courts (HAIPA). The systems are referred to as material banks. The basic principle behind this work is for all the material needed to make decisions to be available to and under the control of the user. The path to all this opens up through the computer terminal.

44. One of the central questions in planning such information systems is, or at least should be, what the law looks like on the judge's screen. This has been given precious little thought however.

45. We now find ourselves having to come to grips with a traditional tension, one that figures more significantly than ever in modern information management: the official informational environment of the average citizen and that of the decision-making power are different. This leads to problems in communication unless what legislation looks like and what an administrative and legal decision looks like can be made compatible. Here, too, official legal signs and a new 'landscape' for law can help considerably. We have the possibility to create a framework for multisensory compatibility.

46. Next we must consider the perspectives of the practical lawyer and the law student. These are reasonably convergent. Laws are supplemented by official materials and other approved legal source material. The difference lies solely in how the information system displays the fundamental matters. The novice and the professional might require different information and different signs for indicating the deep structure of a law. We could get important visual legal experiences.

47. What is also problematic in all this is the use of *acceptable sources of law*. In a constitutional state the informational environment of a judge cannot be a closed one. It should reflect the latest advances that have occurred in legal praxis and the legal literature and offer judge opportunities for proper information retrieval. In this light, for example, the various guides developed by certain Finnish courts of appeal for decision-making in certain areas - child welfare law for instance – are very problematic indeed. They also exemplify the "arm's length rule" often emphasised by *Peter Seipel*. That is, we are easily satisfied with the most readily accessible information. This problem, like many others, could be naturally alleviated in a digital environment by visual warnings.

48. Today's information technology offers singular opportunities to enhance instruction in law. This it could do by providing a visual presentation of legal texts and their deep structure and pinpointing situations where interpretation is required. Back at the 1998 SubTech meeting, when I provided a preliminary and modest sketch of how the principles of data protection could be presented visually using hypertext, how we used computers was a far cry from how we use them today. Today, visual presentation should be part of any computer training. It should be part of the optimal legal culture, which Swedish Professor *Kjell-Åke Modéer* justifiably views as including the infrastructures used by lawyers. The scarcity of law is often a consequence of its infrastructures being underdeveloped.

49. We must get students used to the importance of the deep structure of law from the very outset of their studies. To borrow the very appropriate expression used by Finnish Professor *Kauko Wikström*, the days when many lawyers satisfied or satisfy themselves with the "open the law book" method should be over in the constitutional state. The informational environment of a good lawyer should also insightfully and effectively indicate the deep structure of the law. Traditional texts with their traditional footnotes and other forms of annotation are not always enough.

50. In 1973 a report was published that had been drawn up by a Finnish committee tasked with reforming legal university studies. Among other things, the report assumed that information technology would be taken into use primarily in government and expressed concern that there was shortage of overhead projector transparencies in the faculties of law. Today the last users of transparencies in Finland have retired or close to doing so.

51. But we should be concerned for those who have placed texts – mere texts – in static PowerPoint presentations. Most teachers are using slideshows like traditional slides. Faculties of law are regrettably conservative. Students receive an incorrect impression of the multisensory dimension of law and legal texts.

52. At its best, a legal education gives graduates the skills they need to identify legal problems and to produce a well-reasoned decision written in language that is reflective of our training. More problematic is how that decision, as a piece of communication, reaches the parties, officials and the public at large. Do we need communicatively different decisions that are tailored to different audiences and different purposes? And can it be done visually without the feeling of triviality?

53. It is now time to sum up. I will do so briefly. What I would submit is that it is at last time for us to think of legal communication as a whole. Here we need to combine two questions. The era of the mere linear text should be behind us. We must ask how legal information systems can be designed such that the path information travels – from beginning to end – meets the requirements of the constitutional state. And, at the same time, we must ask what law should look like at the different stages along that path. These are core questions of modern Legal Informatics.

Chapter 4

THE MODERN LAWYER AND HIS ROLE IN THE ERA OF THE INFORMATION SOCIETY AND ITS SERVICES

Arkadiusz Bieliński

Ph.D., University of Bialystok, Faculty of Law, Department of Civil Law, 15-213 Białystok, Mickiewicza Street 1, a.bielinski@uwb.edu.pl

Key words: *information society, information technology, multisourcing, legal services, Legal Information*

Abstract: *This article touches issues related to the transformation of the traditional legal services in an information society service day. It indicates the reason for these changes and their directions, so that the lawyers functioning yet have a chance to stop for a dynamically changing market by implementing the optimal functioning of their office information technology and solutions in the field of so-called legal informatics.*

1. Introduction

It seems that the very title of the article suggests that the material to be presented is complex, but also extremely timely. Already the first part of the title - a modern lawyer and its role could be made the subject of a separate study, because actually the role it plays as advocate or legal advisor has a significant, if not revolutionary change in relation to that with which you could have to deal with a few years ago. Additionally, context, the rear of the modern lawyer in a constantly evolving information society and its services in a relevant and significant impact on contemporary performance of the classic legal profession. It seems that the main driving force influencing the attitude of the modern lawyer is increasingly aware of the client who is waiting for better quality of services, multitasking of law firm and permanent access to legal acts of his interest, expertise and papers and documents related to his case. And all this with a significant reduction in the cost of legal services, which accounted for the lion's share, and probably still account for attorneys' fees. Today's customer has also high expectations associated with the use of tools included in the so-called legal informatics, even allowing free

access to legal services, or the ability to quickly access to the specific records, or the stage of judicial proceedings. Contemporary lawyer or law firm also are increasingly aware that without a revolutionary change (although often this change is intentionally delayed), without departing from the separate settlement of constructing the model, tailored to individual customer expectations for a more universal solution, even management projects concerned with the handling of cases clients, their future is uncertain. Spice all this change adds the fact that many of the innovative solutions that in the long-term dimension probably give a positive effect in the short term are potentially destructive, destabilizing the functioning so far, the classic formula of practice as a lawyer. In this article, I would like to focus on specific issues and indicate some mechanisms of this transformation and indicate the selected institutions that promote the convergence of the modern lawyer with the expectations of the information society.

It is a truism to say that the changes that have occurred in the last few years had a significant impact on the functioning of individuals and social groups, including representatives of the legal profession. The law is instrument which creates a change in the social reality in accordance with the expectations of society and the preferred directions of socio-economic, or it's an instrument to stabilize the changes that have taken place in the social reality, and only secondarily law gives shape to these institutional changes[1]. We can also observe that often determine the status of a lawyer reveals the gap between social expectations and adopted at the level of epistemological assumptions. The source of this discrepancy are multi-faceted, it can be an example way of conceiving responsibility for law[2]. Information infrastructure is changed from stage oral communication through the writings era on information technology ending. As part of this technology reaches a certain gap, namely, there is a noticeable delay occurring between data processing and knowledge processing. Data processing is the use of technology to acquire, reproduction and dissemination of information, knowledge processing is however a set of technologies that help analyze, select and organize the data created, making it easier to deal with them. Data processing by far outstripped processing solutions for knowledge. However, you can observe that the distance separating them is reduced, and when will disappear, society will be in the information society[3]. This raises the question of how lawyers behave in relation to new systems, to modern information technologies? The source of the

[1] E. Łojko, *Role i zadania prawników w zmieniającym się społeczeństwie. Raport z badań*, Warszawa 2005, p. 93.
[2] See P. Kaczmarek, *Tożsamość prawnika jako wykonawcy roli zawodowej*, Warszawa 2014, p. 33. See also M. Zirk-Sadowski, *Uczestniczenie prawników w kulturze*, Państwo i Prawo 2002/9.
[3] R. Susskind, *Koniec świata prawników? Współczesny charakter usług prawniczych*, Warszawa 2010, p. 28.

answer to this question can become analysis of the expectations and preferences of customers[4]. It is reported by the customer demand for new working methods and increase the efficiency of firms will eventually lead to the implementation of new technologies[5].

2. Expectations of customer's market of legal services

First of all, there is a gap in terms of the commercial interests of law firms and their clients. Because the client expects that the situation will be resolved quickly, without excessive time commitment lawyer, and therefore the fee payable will be reduced to a minimum. Law firm while counting on a complicated job, requiring considerable commitment, binding, of course, with high fees. Is using these expectations can thus rely on a solution that would seek to break the obvious asymmetry? It seems so, although the law firms that seriously wonder about modernization must take account of certain factors that may hinder the implementation of this model. Reference is made to two such threats - problems with empathy lawyers and hourly billing. The first of the threats is characterized by the fact that for a lawyer is often hard to understand what the client wants to tell him, and understand his situation and the operating conditions (this is particularly complex for the functioning of organizational structures). Focuses more on proposing reasonable from his point of view, ignoring resolve customer expectation empathy in his situation, resulting for example from the function of a lawyer of the legal department of the company. The second risk is more rooted and hard to convince lawyers to withdraw from hourly billing system for their work. Despite many initiatives pointing to alternative billing, settlement hourly further provides a solution model. It should be clear that as long as it does not change, you can forget about the process of matching the commercial interests of the firm to the client's interest. Could it be that a change in this area was so unfavorable to lawyers that justified their reluctance to change in this area? By Richard Susskind indicating that what initially may seem like a simple way to self-destruct in practice this is not necessarily true, because technically perfect with sharing an office with its customers enthusiastic to minimize the involvement of lawyers and legal costs in the medium and longer term would begin to draw complex and highly valuable tasks, which sooner or later must confront each company[6].

[4] I make no distinction here on corporate and individual customers, because actually occurring differences in their expectations, they have been many common areas.
[5] R. Susskind, *Koniec świata prawników?...*, p. 33.
[6] R. Susskind, *Koniec świata prawników?...*, p. 146.

Another reason for the asymmetry on the axis law firms - the customer is a mismatch between the expected way to provide legal advice and the final result. A traditional lawyer will offer traditional, personalized advisory service settled hourly often leading to present complex and inefficient legal opinion, which the client is not able to understand. While the client expects matching possessed by lawyers' expertise to his situation. In other words, in terms of initiating mechanism of transforming knowledge into value for the customer that is relevant. Lawyers must therefore in their work expect to use knowledge management systems to help find cheaper, faster, simpler, highly qualified solutions tailored to customer expectations. As an example of such an innovative approach can point to KPMG, which defines its relationship with the client and that the mission in relation to it is to implement: „By bringing different perspectives, sound judgment and extensive cross-border collaboration, KPMG professionals help to enable clients' informed decision-making wherever they do business and no matter how far-reaching their operations[7]."

Customers (especially corporate) often want to have real-time access to information, data related to the conduct of their affairs by law firms[8]. Seemingly, the problem does not exist if one conducts legal services office. Increasingly, however, so that such a service is divided between several dozen law firms, each of which carries its own portal, a website to which you need to be logged in to get the necessary information. Instead, clients expect one place which will flow information from all the cooperating firms in a fixed format. From the point of view of the office this solution is not attractive, mainly due to the need to tediously enter data for each client systems required by the format. An example of such a system is Anaqua introduced by the Ford Motor Company and British American Tobacco[9].

Currently customers (even if they not fully aware of this issue) also begin to depend on to avoid legal disputes everywhere where possible. They are interested in this, that in exchange for a lump sum pay the most, lawyers and law firms managed really the risk of legal dispute arises, analyzing the situation of their client in this particular angle. Lawyers, while primarily interested in long, complex, and thus costly for the client, litigation. Richard Susskind gives a very suggestive example of Cisco, that hiring an external law firm for legal services had resulted in placing reducing the cost and time spent on disputes law firm brought a radical change in the nature of its engagement with the customer. It turned out that both the firm and the client want

[7] http://www.kpmg.com.
[8] This mechanism is called the sharing of data.
[9] http://www.anaqua.com.

to avoid disputes. Law firm therefore decided in addition to the traditional manual disputes the introduction of management of legal risk[10].

Customer expectations, in particular, the individual, the act of obtaining legal advice[11] by him can be imaged using a cycle consisting of three processes. The first is to recognize - citizens or clients realize that in the circumstances in which they find themselves, would benefit from legal advice. The second process is the selection - citizens or customers choose to find a source of legal advice that might be helpful in this situation. The third element of this chain is a service, which is just receiving legal advice[12]. Question may arise where the space for the modern lawyer, legal information systems if classic activities potentially satisfy each of the identified elements? Nothing could be further from the truth. Classic lawyer with respect to the first element, determines that the client came too late and it will be hard to help him; with respect to the selection target will be called command lawyer whose services have someone previously used (does not have to be all highly qualified lawyer); regarding the services it currently takes the form of tailor-made settlement and billing hourly time lawyer. Ensuring greater access to legal services, often free of charge for example: open-sourcing of these services, portals containing legal information, online portals will affect the realization of citizens that the law has an effect on him, causing identify at an early stage needs use of legal advice. Second, with the development of electronic legal services market will grow the number of potential beneficiaries to address the need to provide legal advice and, therefore, citizen get a real opportunity to select the entity that ultimately give him this advice. Slowly begin to appear portals that allow you to compare the services of law firms based on different criteria. The third aspect, that is, to provide the same services in the face of growing competition, expanding the number of suppliers (both legal and alternative business entities providing legal services) will cause that legal advice will be cheaper, faster and more affordable in terms of content. This phenomenon can be called multisourcing of legal services.

3. Technological trends in the legal services industry

In addition to the expectations of the customer on the development of the model of the modern lawyer and tools used by him in the field of legal informatics are also affected by the phenomenon, which collectively can be described as trends in technology. Directory of these phenomena is certainly not closed, but it's possible to try to identify in my opinion the most

[10] R. Susskind, *Koniec świata prawników?...*, p.149.
[11] Collectively, this mechanism could be called the law and access to justice.
[12] R. Susskind, *Koniec świata prawników?...*, p. 225.

important. Perhaps the most far-reaching importance is aware that the information technology, an essential tool in the work of a lawyer does not have its border development. So you can not stop at a certain point of innovation stating that in this regard has already been achieved everything and this state of affairs will continue for a long time. This approach is absolutely wrong, it is expected to have finger on the pulse when it comes to the development of IT technology, while being aware that technology will change jobs much faster now than it was before.

Another phenomenon is also striving to achieve information satisfaction, which is brought to us the information exactly matched to our expectations. In addition to the global Web search using the available search engines to help you find the information of interest to us, this satisfaction information also applies to business law firms. Because the client expects to obtain only the legal information available only to those documents on which it depends for the moment.

We should also be aware of what can be called the Internet community, in which arise new ways of interaction and cooperation. This community is divided by Richard Susskind into four areas: communication, production and collaboration, networking and community building, trade and exchange[13]. From the point of view of the modern lawyer, communication issues have an important role (in addition to traditional e-mail gaining popularity all kinds of instant messaging, video call or video conferencing). In terms of the production may play an important role technology called "wiki"[14] that allows you to directly modifying and supplementing websites by the users themselves. Therefore, it can also be used to share knowledge of the law, both between offices, as well as between law firms and clients. May provide a common platform to debate and discuss the information that is posted on the website. The last issue related to the information society as well as the modern lawyer is a networking and community building. It cannot be longer ignore the increasingly growing importance of social networking sites[15]. They can be used to make business contacts and create professional community.

Trend, having great importance from the perspective of the creation of the legal services market, it is also the realization that we now have to deal with the increasingly dynamic growing group of people belonging to the so-called Network Generations. These are people for whom access to the Internet, the use of modern communication technologies, access to the media, social media activity is something quite natural inscribed in their lives. They do not know any

[13] R. Susskind, *Koniec świata prawników?...*, p. 75.
[14] The best-known site of this type is Wikipedia.
[15] Facebook or Linked-In - more professional social networking site.

other alternative method of communication, because they were born in a time[16] when traditional communication techniques have lost their importance. And this network generation will determine future trends affecting the shape of the legal profession because the people belonging to this group will be the lawyers and clients of tomorrow[17]. They will not be interested in the classic methods - direct contact by lawyer with the client to transfer personal knowledge. They choose their natural communication channel - the Internet in order to obtain legal advice, often replacing personal contact videoconferencing connection. A relatively new phenomenon is the provision of legal advice online.

4. Factors influencing the changes in the legal services market

From the above discussion it is clear that changes are inevitable. Richard Susskind identifies three major factors to these changes: the challenge of "more for less"; liberalization of the legal services market and the development of information technologies[18]. He has already been mentioned that customers are beginning to expect greater efficiency in serving their lawyers, while cutting costs for legal services. So what to do? You can implement the so-called efficiency strategy that gives the opportunity to reduce operating costs, and law firms to propose alternative ways of settling legal services. In the long term, it may also become the use of so-called strategy for cooperation in the consolidation of customers (primarily operating in the same industry) in order to obtain legal information that is common to them. This would replace the currently functioning formula provides a very similar, if not identical, the data separately for each of these customers. Of course, from the point of view of legal office is not preferred, because the previously rendered multiple times, the repeat service can be offered only once. From the customer's point of view, this solution is beneficial to contribute to a reduction in legal costs[19]. The liberalization of the legal services market is slowly becoming a reality. It is true that slowly but noticeably but this kind of service is no longer exclusively the domain of professional lawyers. Increasingly, we are dealing with so-called alternative business service providers who under certain conditions may provide legal aid or investment in law firms by people who come from outside the circle of lawyers. As to the third cause of change, the development of information technology, probably does not need to convince anyone. Lawyers

[16] The year's border separating people who remember a world without the Internet and network generation is the year 1985.
[17] R. Susskind, *Koniec świata prawników?...*, p. 89-90.
[18] R. Susskind, *Prawnicy przyszłości*, Warszawa 2013, p. 25.
[19] R. Susskind, *Prawnicy przyszłości...*, p. 42-44. He gives the example of a tool based on this strategy – Rulefinder prepared by the law firm Allen & Overy - management of legal risk.

and their forward-thinking clients feel the inevitability of changes in their functioning due to the development of IT technology. Only incorrigible optimists, or just short-sighted people may argue that these techniques, if at all, only to a small extent will affect the functioning of the existing lawyers.

5. Summary

It's fair to say that the current model of functioning in the next 15-20 years will change dramatically. This applies to the functioning of both law firms, lawyers working in the legal departments of companies, as well as individual lawyers. The current customer market will also change primarily for the reasons described above. Perhaps only a few big law firms manage to survive in close to the current form, but they will have to undergo fundamental changes. Quiet about their future can also be a tiny group of highly specialized experts, while other subjects must introduce these changes in order to survive in the market. Therefore, necessary to divide the whole process of handling the matter into smaller separate stages (decomposition), in order to determine which of them actually require the participation of a lawyer, and which can be delegated as an alternative means of obtaining services through other entities. A catalog of such alternatives is given by Richard Susskind, which I cite without a broader discussion of referring in this regard to the publication of this author used in this article. He points to the following: obtaining internal (in-sourcing), (de-lawyering), relocation, offshoring, outsourcing, sub-contractors, joint sourcing of services (co-sourcing), nearshoring, hire lawyers (leasing), remote cooperation (home- sourcing), the public access (open-sourcing), community involvement (crown-sourcing), computerization, obtaining individual performers (solo-sourcing), dispensing with the services (no-sourcing)[20]. Such dislocation in the conduct of affairs gives you a starting point to a mechanism of multisourcing of legal services, or their acquisition from multiple sources. In this case, the role of the firm will be able to be limited to the management of the project, to harmonize all processes in one product, which will eventually be presented to the client. Lawyers cannot avoid the phenomenon called commoditization, or abandonment services model tailored to the individual client, to the more universal solutions, which can be used by a larger group of customers. This involves the process of standardization of certain repetitive legal actions (the typical provisions of contracts), their systematization and packaging, or sharing (also free) outside parties over the Internet. Modern lawyer is an entity combines both traditional provision of legal services to the techniques that use information

[20] R. Susskind, *Prawnicy* przyszłości…, p. 60.

technology. This is a lawyer who is ready to settle disputes so-called Internet ODR - Online dispute resolution, which is the most popular e-mediation, e-negotiations. Lawyer, who works in information society days is characterized by multidisciplinary information society, the ability to find niches in the market, allowing for specialization, openness to customers and their expectations, as well as cooperation with other lawyers in the market. To some extent, therefore, survival will depend on whether the firms will be able to "come up again," and acquire new skills to be able to provide tailored to a higher level of competitiveness of legal services[21].

The above-mentioned aspects related to the role of the modern day lawyer information society development also apply to lawyers acting for the Polish market - so these corporate and individual. Perhaps out of large, often international legal offices, in which some mechanisms to ensure their competitiveness in the future, are slowly being implemented, most of the moves of each need to change the approach to customer expectations and the implementation of revolutionary information technologies. They prefer to work with a mechanism for individual services, sewn to measure, focusing on the provision of services in the traditional form. Such a passive attitude may, however, in the near term, lead to their demise, while promoting those entities that at the appropriate time in advance invested in the transformation of their services and become strong competitors in the fight for a huge market of legal services.

[21] R. Susskind, *Koniec świata prawników?...*, p. 239.

Chapter 5

THE NEW
INFORMATION SOCIETY CODE OF FINLAND

Rauno Korhonen

Professor of Legal Informatics, University of Lapland, Faculty of Law, Institute for Law and Informatics, PL 122, 96101 Rovaniemi, rauno.korhonen@ulapland.fi, www.ulapland.fi

Keywords: *Legislation, reform, legal politics, communication law, information law, legal informatics, ICT-Law; law and informatics.*

Abstract*: The Information Society Code as a new act replaced recently eight former acts in Finland in the field of communications. The amount of sections in this one single act is now about 350. The aim of the short paper is to analyze the challenges and benefits of this kind of legal politics.*

1. Introduction

The large reform of legislation applying to electronic communications has recently been under the work-process in Finland. On January 2014 Finland´s Government submitted its proposal for Information Society Code to Parliament. In accordance with the Government Political Programme, the key provisions that apply to electronic communications have been integrated in the Information Society Code. After overlapping items were removed and provisions were consolidated, *Information Society Code (917/2014)*[22], which came into force January 1st 2015, now consists of 350 sections, whereas there were previously 490 sections in eight replaced acts.

The purpose of the Information Society Code is to ensure that electronic communications services are available throughout Finland. The services must be technologically sophisticated, safe, easy-to-use and reasonably priced. Legislation will also be used to create better than ever

[22] An unofficial translation of Information Society Code in English can be found from the web-pages of Ministry of Transport and Communications in Finland: http://www.lvm.fi. Choose first "Tietoyhteiskuntakaari" and then a link "Legislative drafts Finnish Information Society Code 31.3.2014". The name of the act is *tietoyhteiskuntakaari* in Finnish language.

conditions for competitive business, development of and innovations in communications technology.[23]

One starting point for the development of new rules in Information Society Code is that according to *The Constitution of Finland* some basic rights and liberties are protected by the section 10:

"Everyone´s private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.

The secrecy of correspondence, telephony and other confidential communications is inviolable."

Almost similar rules can naturally be found for example from *the European Convention on Human Rights* and from *the Charter of Fundamental Rights of the European Union*.

2. The Reformed Legislation

The following acts have been replaced by the Information Society Code since January 1st 2015:

Communications Market Act (393/2003)[24]

Domain Name Act (228/2003)

Act on the Protection of Privacy in Electronic Communications (516/2004)[25]

Act on Provision of Information Society Services (458/2002)[26]

Act on Television and Radio Operations (744/1998)

Act on Radio Frequencies and Telecommunications Equipment (1015/2001)

Act on the Prohibition of Certain Decoding Systems (1117/2001)

Act on Auctioning Certain Radio Frequencies (462/2009)

Because of the remarkable amount of relatively important acts, this reform causes fast challenges for re-education in private and public sector and also for the updating of legal commentary literature in Finland.

---

[23] Section 1; Objectives of the Act: "*This Act endeavours to foster the supply of electronic communications services and to ensure the availability of communications networks and services at reasonable conditions throughout the country. A further objective of the Act is to secure the efficient and uninterrupted use of radio frequencies, to foster competition, and to ensure that communications networks and services are technologically advanced, of high quality, reliable, safe, and inexpensive. Another objective of this Act is to ensure the confidentiality of electronic communication and the protection of privacy."*

[24] Communications Market Act was the largest of these replaced acts with about 160 sections.

[25] This act was based to the Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

[26] This so called eTrade act was based to the Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

3. The Structure of the Information Society Code

The Information Society Code, which is in the Finnish legislation hierarchy the normal act, consists of XIII parts and 45 chapters. The Parts are following:

PART I GENERAL PROVISIONS

PART II TELECOMMUNICATIONS SUBJECT TO NOTIFICATION AND LICENCING

PART III IMPOSING OBLIGATIONS AND UNIVERSAL SERVICE

PART IV FREQUENCIES AND NUMBERING

PART V RIGHTS OF SUBSCRIBERS AND USERS IN CONNECTION WITH COMMUNICATION SERVICES

PART VI CONFIDENTITALITY OF COMMUNICATIONS AND PROTECTION OF PRIVACY

PART VII SPECIAL RULES APPLICABLE TO ELECTRONIC SERVICES

PART VIII AUDIOVISUAL SERVICES AND RADIO OPERATIONS

PART IX COMMUNICATIONS NETWORKS, SERVICES AND EQUIPMENT

PART X MEASURES TO ENSURE THE CONTINUITY OF COMMUNICATIONS AND SERVICES

PART XI AUTHORITY FEES AND COMPENSATION

PART XII ACTIVITIES OF AUTHORITIES

PART XIII OTHER PROVISIONS

4. Some Headlines concerning the Reform

Consumer protection has been improved in Information Society Code compared with former rules. In case where consumers order and pay for products and services via their mobile phone, it has been ruled that telecom operators and the companies selling the said products or services would share accountability. This means that in addition to the seller or service provider, consumers could turn to their telecommunications operator if the service or product is faulty or the consumer never receives it or is unable to discontinue a service order.[27]

[27] Look for example the press release of the Ministry of Transport and Communications: *Information Society Code to Parliament.* Press release 30.01.2014. Http//:www.lvm.fi/pressreleases.

More detailed information can be found from the Government Bill (*HE 221/2013 vp.*) concerning the Information Society Code. Government Bills are officially drafted and published only in Finnish and Swedish. Swedish is the second official language in Finland.

Special attention has been paid to *protection of privacy* and *information security*. Provisions applying to protection of privacy and ensuring information security would be extended to cover all operators that convey communication. The provisions would apply to such matters as confidential messages exchanged via social media.

Major changes faced in *the media sector* have been taken into account in the proposed new operating license system. The system has been simplified by transferring a significant part of decisions concerning radio and television programming licenses to the *Finnish Communications Regulatory Authority* (FICORA). In future, new frequency bands that will be utilized for mobile communications could be distributed via auction.

Steps will be taken to make monitoring of the pricing used by companies that hold significant market power more effective. Above mentioned FICORA can, for example, be given the right to determine *a maximum price* for a telecommunication operator´s wholesale product when problems with competition arise.

The integrity of communication services will be promoted by creating better conditions for cooperation between the operators and the *authorities in controlling* disturbances. The most important network control centres and other critical systems should be maintained so as to allow them to be restored to Finland immediately in the event of special circumstances.[28]

5. Some Critical Observations

Some critical observations concerning the new act called Information Society Code must be done if we want to take into consideration the demands of the modern Rule of Law State. It has been used to say in Finland that there are following specific *general principles for the basic legal information sources* of Constitutional State: availability, rightness, reachability, searchability, understandability, usability and low price.

Does the new Information Society Code with about 350 sections fulfill for instance the requirements of the understandability –principle? *Understandibility* could be explained to mean that *official legal information sources*, as law-texts, should be easily understandable for most of the citizens, not only for lawyers. The texts should be clear as itself or by using some helping tools, signs and clarifications made by the information producers.

This kind of huge act can also be seen as a result of so called *Juridification* –phenomenon, which means according to some legal scholars that societal progress where more and more

[28] Look also *FICORA will have more tools for steering and supervising electronic communications*. Published 7.11.2014. www.ficora.fi; News 2014.

things in society are ruled by the law. The expansion of norms and all the time rising amount of acts and rules are some elements of juridification.

What about then in this context the common principle of western countries that even an ordinary citizen has duty to know the basic legislation? And this despite of the lack of legal education. So, he or she cannot for example say that: "Sorry, I didn´t know that it is not allowed to do this or that according to the law."

The Finnish politicians have very recently discussed about our problematic situation where the legislation and the amount of rules in many cases is a kind of obstacle for the economic growth, for new innovations and for the productive and creative work. Our politicians would like to see less legal bureaucracy in the society.

If the answer for these problems will be in future more and more large "monster-acts" like Information Society Code, which replaces the several smaller ones, this progress should be first analysed very carefully before the final political decisions.

Finland has been a member of European Union for about 20 years. According to some studies and statistics the amount of Finnish rules is now more than double compared with the situation when Finland was negotiating about the membership-requirements in 1994. According to the same studies the main reason for this legislative progress has been EU – it´s regulations and directives. For this reason the EU has sometimes been called as "Legislative Factory" by some sceptical observers.

EU has also had another kind of influence to our legislation. It is typical for new acts that they contain a lot of definitions of concepts, which are important for the applying of those acts. For example, the section 3 in the Information Society Code contains even 43 different definitions of concepts for the purposes of that Code. The growing number of definitions has been typical for EU-legislation and this legislative politics has changed our national acts. For instance, our *Personal Data Act* (523/1999), which is also relatively technically oriented act, contained originally only 9 definitions.

The following list of the titles of concepts in Information Society Code is long, but it tells a lot of about the meaning and scope of the act, even without the explanatory content of the concepts:

Section 3 Definitions

1) Audiovisual programme;
2) Audiovisual content service provider;
3) Internet connection service;
4) Mass communications network

5) Cable duct
6) Fixed installation
7) User
8) Related service
9) Related operations
10) Value added service
11) Terrestrial mass communications service
12) Programme
13) Amateur service
14) Radio equipment
15) Radio frequency
16) Radio broadcasting
17) Radio communication
18) Location data
19) State of establishment
20) Sponsorship
21) Protected name or trademark
22) Electronic communication
23) Telecommunication equipment
24) Teleshopping
25) Telecommunications terminal equipment
26) Television broadcasting
27) Telecommunications operator
28) Information security
29) Information society service
30) Subscriber
31) Subscriber connection
32) On-demand audiovisual media service
33) Safety radio communication
34) Network service
35) Domain name
36) Communications provider
37) Communications service
38) Communications network equipment

39) Communications network

40) Identification information

41) Corporate or association subscriber

42) Universal telephone service

43) Public communications network

6. Concluding Remarks

It is a common phenomenon in Finland as a small country (5.3 million of inhabitants), that the amount of specialists on each special law field is very limited. For this reason, sometimes the only legal commentary of new act is published by the same persons who have drafted and written the act in some ministry. Same persons very often too visit Parliament committees as experts in order to give supporting statements for law-making work of the members of parliament.

During the last about 10 -15 years the Ministry of Justice in Finland has made a lot of efforts in order to improve the quality of Finnish legislation. There is for example right now working the special organ: *Government´s Law Drafting Development Group.* The results of this and other important projects will be seen in future.[29]

[29] Look the web-pages of Ministry of Justice: Entry page > Operations and goals > Legislation and the development of legislative drafting > Better Regulation > Development projects.

Chapter 6

LEGAL CONCEPTUALISM GENERAL THEORY OF LAW – A NEW METHOD OF STATEMENT OF THE LAW AND A WAY OF EXPLAINING APPLICABILITY OF LAW

Jakub Rzymowski

Ph.D, University of Łódź,. Faculty of Law and Administration, Department of European Economic Law, rzym@prawokomputerowe.pl

Keywords: *general theory of law, legal conceptualism, normativism, statement of the law, applicability of the law*

Abstract: *The article discusses a new theory of applicability and statement of the law — legal conceptualism – general theory of law. The legal conceptualism – general theory of law is a development of Aristotle's and Abelard's views on universals regarding the law. Simultaneously, the general theory of law is able to replace the Kelsen's theory. The general theory of law can be either a common denominator to numerous theories of applicability of law known so far.*

The general aim of a text is presenting a theory which in my opinion should be named as "legal conceptualism"[1] or "conceptual theory of applicability and statement of the law", or "general theory of law". The second aim is to present reasons which led to coming this theory into existence.

The theory being proposed is an attempt to transfer some of views on universals – universals on law. This theory is able to replace theories known so far, it can be their supplement and it also can be their common denominator.

[1] The more detailed explanation why I named this theory in this way one can find in the further part of text.

1. The essence of theory

1.1. The statement of the law

As far as the essence of theory is concerned, the easiest way of explaining it is to start from considering a phenomenon of regulation.

The existence of regulation in a legal act is unquestionable. The regulation is a linguistic phenomenon due to which one knows which right is entitled to whom. In the process of statement of the law one refers to the meaning of words being included in a regulation and that is how one establishes its meaning — one finds to whom which right is entitled to[2].

1.2. The applicability of the law

I consider writing down a right in a regulation as insufficient ground to state the existence of this right. In my opinion the right exists as it exists beyond the regulation, in reality and in a human mind. A human being understands the existing right by using his or her mind. A human understands the fact of right's existence.

I pay attention that the mind involves the right in itself as it understands it but it does not create it. The right is a human's attribute. Just like his or her height, age or beauty.

Applicability of the law can be reduced to an answer to a question "Why does the law exist?". If one considers the law as a set of rights entitled to particular persons and that is my opinion, then the applicability of the law reduces to an answer to a question "why does a particular right exist?"

The right written down in a regulation exists, as the regulation does not refer to emptiness but to the right placed in a wise human mind. Strictly speaking, a regulation refers to a right placed in wise minds of lots of people. I pay attention in the same time that the mind involves the right because it understands it but does not create it.

The right is a human's attribute. Just like his or her height, age or beauty.

My theory has been presented above, further considerations in the text are a description of the way of concluding a concept, specifying it and indicating possibilities which it offers.

2. Causes of coming the theory into being

Aristotle claimed (I quote after W. Tatarkiewicz[3]) that philosophy came into being out of admiration. W. Tatarkiewicz added that except that, there is the second kind of philosophy, the

[2] In order not to complicate my line of reasoning I omit the issue of obligation.
[3] W. Tatarkiewicz, *Historia filozofii*, Warszawa 1958, p. 10.

philosophy which came into being out of distrust[4]. The aim of philosophy of admiration is to understand and describe. Working according to philosophy of admiration is of positive nature[5]. The aim of philosophy of distrust is criticism of misconceptions. Working according to philosophy of distrust is of negative nature.

When I look at philosophy, I do not notice it from a historian's of philosophy point of view who describes what had happened. The philosophy "is" to me. Legal conceptualism – the general theory of law formed due to philosophy and that is why among others and also why, to explain it better, I present below what philosophy is to me. The philosophy is not a kind of science like history or history of philosophy for me. Obviously, one usually recognizes philosophy in historical terms. In such a way it is at least explored at the beginning. One learns information about philosophers, where did they live and created. First and foremost, one finds out what did they create. Despite recognizing philosophy in historical terms, to me, the philosophy is a quite different field of science from history. The history describes what had happened. The philosophy describes what is happening. Particular concepts used by philosophers formed in a certain moment of the past, however they do not belong to the past in one's point of view. The concepts formed in certain order, as that is just how the world looks like — people are born and they die and in the meantime some of them put a building brick to a huge philosophical structure. When one looks backwards and sees all these bricks — they are. They are here and now. They are ready to use them for one who wants to use them and to build something new. Perhaps my approach to philosophy is unprofessional. I emphasize that I am not a historian of philosophy nor its scholar. I do not examine philosophy. I am exploring philosophy and I use it. I have got more to say. I think that such an approach to philosophical output is proper. I believe this is what the philosophy is for. It is alive and accessible. It waits for next people to use it.

2.1. There is the distrust at the heart of my intellectual sources.

I do not trust normativism as a theory of applicability of the law. The source of this distrust is a doubt regarding a fundamental norm — and thereby a doubt if normativism explains the applicability of the law. The source of this distrust is also a doubt regarding existence of any norm — thus a doubt if normativism indicates how to make the statement of regulations.

I do not trust a concept of religious natural law. The source of this distrust is a doubt regarding a possibility of recognizing the intention of a law giver, a certain Higher Being, a

[4] W. Tatarkiewicz, *Historia filozofii…,* p. 10.
[5] W. Tatarkiewicz, *Historia filozofii…*, p. 10.

Supreme Being called for example a god[6]. I take no account herein to an issue of this Being's existence, I just signalize a doubt as to a possibility of real and well-aimed recognition of its intention. If intentions of the Supreme Being are unrecognizable or partially recognizable, then the missing parts and perhaps the missing totality are supplied by persons who state that they have learnt these intentions. I consider reading the source of law into such supplements as ridiculous.

In my opinion, a concept of secular natural law is more serious and more honest for certain. I think that the idea of deriving human rights and obligations out of human nature is not futile, however as I wrote — it is an honest one. I do not know if deriving the law out of human nature is possible. Nevertheless, those who try to do this deserve respect. They have got nothing more than the work itself to legitimate their work. My distrust herein is less and its source is a doubt regarding a possibility of deriving all the rights out of human nature. And again I am worried if loopholes are being completed with making up. I do not know if that is the case but I am distrustful.

I am distrustful towards legal positivism as well. The distrust towards positivism towards crimes committed by Germans and Russians during and around The Second World War. Though, I believe that distrust towards positivism which source is an unbridled horror of Germans and Russians is a simplification of a problem. My distrust towards positivism also arises on the ground of doubts if one can find the grounds of applicability of the law in his or herself. I referred to the fundamental norm above. The rule of recognition presented by Herbert Lionel Adolphus Hart does not convince me either. It does not convince me because in my opinion the rule of recognition is nothing more than the fundamental norm but only named in a different way[7].

The philosophy of distrust is the philosophy of criticism. It is easy to criticize. It is easier to criticize someone's view than present one's own. I do not avoid indicating the sources of my varied distrusts in my struggles. I do not avoid but criticism is not the aim of my work. My aim is to present a new, different approach. To present the approach referring either to the applicability of the law and to the statement of the law. If I criticize someone's views, it does not mean that they are wrong. I just have doubts if they are well-aimed. The philosophy of

[6] Against the accepted tradition I write the word “god” using a lowercase letter, not a capital. I am aware of that as I do not refer in my considerations to the God of Old Testament known as Yahweh nor to the God of New Testament. I treat the word “god” as a generic noun, not as a proper noun. Generic towards a category of existences to which one can involve god Yahweh, god Brahma, god Amon, god Odin, god Zeus.

[7] I do not develop this view due to lack of space and the subject matter of text, however it has been a while since I suspect that H.L.A. Hart's concept is a concept of H. Kelsen but only transferred into the world of different terms, in which a norm is a rule, and a fundamental norm is the rule of recognition.

distrust only gives me encouragement to work. I perceive my own work as the philosophy of admiration. Presumably, words about admiration may seem ridiculous but I use them for the reason that W. Tatarkiewicz used them to define a kind of philosophy which aim is to understand and to describe. I try to understand and then to describe what I have understood. I am going to convince to my beliefs those who are reading these words and make them follow me.

2.2. Doubts regarding normativism and a direct cause of coming the theory into being

The proposed theory is an attempt to transfer some of views on universals — universals on law. This theory is able to replace theories mentioned at the beginning, it can be their supplement as well or even a common denominator. I admit that the proposed theory arose mainly on the grounds of normativism. Normativism is a convenient theory. Convenient but well-aimed only when one considers it as well-aimed. Normativism is well-aimed when one believes in it. When one does not believe in it, normativism seems faulty and what is more — unnecessary. Normativism is coherent but only when one looks at it from inside, by accepting it as one's own, one recognizes its trueness and coherence. Normativism is like religion but also as a disease. The disease of normativism lasted long to me. I used to operate a term of norm while I was writing my PHD thesis. Eliminating the subject matter of PHD thesis which is not crucial herein, I add that the thesis is full of detailed considerations. In my study I analyzed regulations and their groups in fact, and step by step, slice by slice I was establishing the content of norms and next I was setting up who has got which obligations and to whom which rights are entitled to.

I was infected with normativism. When I look at it now I can state with full responsibility that in spite of being ill for many years, symptoms were not intensified. When I remind myself how I used to explain my non-academic students different law issues I realise that I regularly started from analysing a regulation. I presented the regulation just by projecting it on the wall and then I explained which rights and obligations result from it and who they concern. Obviously, it was quite frequently not only one regulation but a few and I projected them one after another discussing them and if it was possible, I used to project them equally — compressed on a slide and I was discussing them. I used to present regulations but I was talking about rights and obligations. I did not do it as a result of careful reflection, rather by dint of saving time during the lecture. Elimination of a stage of establishing the content of norm during the lecture allowed me saving time and thus passing on a larger amount of information. In this

way, saving time protected me from strong escalation of symptoms of a disease called normativism. At the same time, quite unconsciously, I used to eliminate a stage of establishing the content of norm during the statement of law. Thereby, somewhat by chance, I discovered that norms are unnecessary to make legal explanations.

The disease lasted many years, however by dint of small escalation of symptoms, my recovery was fast.

After my PHD thesis defense I was honoured to talk for several hours with one of the reviewers, professor Zdzisław Brodecki. During this talk, which turned out to be crucial to me, the conversation started to concern norms. I do not remember which detailed issue the conversation was devoted to at that moment, but when I am making an effort to remind myself, it seems to me that we have been talking about general issues and I remember that this fragment of conversation was focused on different concepts of principles of law. When I interjected something about norms, then professor Z. Brodecki said some words which have stuck in my mind and resulted among others in the present text. I quote professor's Z. Brodecki words although I do not quote them accurately as I quote them using just my memory. Therefore, when I said something about norms, professor Z. Brodecki said: "The norms do not exist". Then I asked what does exist if there are not any norms and professor Z. Brodecki added: "The norms do not exist, there are rights. There are rights and obligations and in fact there are only rights".[8]

3. Occam's razor

I pay my attention that an assumption that norms do not exist is consistent with known in philosophy principle of economy formulated already in the 14th century by William of Ockham. The Ockham's version of this principle is as follows: "Plurality must never be posited without necessity".[9] Necessity is understood herein as the necessity to make the statement of a regulation. Plurality posited beyond that necessity are: a regulation, a norm and a right. As a concept of norm is non-essential to set up the content of right, it is unnecessary, and as it is unnecessary it becomes removed from a line of reasoning with "Occam's razor".[10] To continue Ockham's principle it is worth quoting a sentence by L. Kołakowski related to Ockham himself. The sentence is: "Let us think what is really necessary to understand the world"[11]. This sentence

[8] Professor Z. Brodecki cured me from my disease and made my considerations possible. Nevertheless, I emphasize that inasmuch Professor gave me a cure, showed me the way and made creation of theory possible, I owe him coming the theory into being but one can blame only me for its details, shortcomings, simplifications.
[9] After: L. Kołakowski, *O co nas pytają wielcy filozofowie. Trzy serie*, Kraków 2008, p. 95.
[10] For further details see: L. Kołakowski, *O co nas pytają…*, p. 95.
[11] L. Kołakowski, *Ułamki filozofii*, Warszawa 2008, p. 53

suggests a similar one, namely that one should think what is really necessary to understand the law. When one thinks about it then he or she concludes one simple sentence. Norms are not necessary to understand the law.

4. The statement of the law

In the proposed method of statement of the law I begin my considerations from a regulation as a linguistic phenomenon. The nominalistic attitude presented in the Antiquity by stoics[12], in the Middle Ages by Roscelin[13] of Compiegne and initially by Peter Abelard[14] is insufficient to carry out the process of statement. As one should recognize according to nominalism that the rights included in regulations are only creations of oration, of language. I accept an attitude of Peter Abelard herein, known as sermonism. According to this attitude, universals [belong to the language (...) as sounds with meaning][15].

Particular stages of the statement have got, in my opinion, the order described further. A regulation has got a content consisting of words, words have got meaning, by knowing the meaning of words one learns the meaning of a regulation, by knowing the meaning of the regulation one reads which rights are written down in it.

5. The applicability of the law

A question should be asked if talking about specific rights understood as rights resulting from specific regulations or understood as rights resulting from groups of regulations, one does not refer to the emptiness. Well, one does not.

I believe that the right written down in a regulation exists, as the regulation does not refer to emptiness but to the right which already exists. The right just exists, it has not been created or set. This right is understood by a wise human mind. Strictly speaking, the right is understood by wise minds of lots of people. A regulation is a linguistic phenomenon, a legislator's note[16] of technical nature. This note is necessary because nowadays it is impossible to pass on the law by oral tradition. Plato's ideas cannot be cognized by senses but can be cognized only by mind. Ideas can be thought, they can be described by the mind when their copies[17] are noticed. It is quite similar with rights, one can describe them using the mind when their reflections in a

[12] W. Tatarkiewicz, *Historia filozofii*..., p. 171.
[13] W. Tatarkiewicz, *Historia filozofii*..., p. 319.
[14] W. Tatarkiewicz, *Historia filozofii*..., p. 321.
[15] W. Tatarkiewicz, *Historia filozofii*..., p. 321.
[16] I heard this or a very similar definition from professor Małgorzata Król.
[17] K. Twardowski, *O filozofii średniowiecznej wykładów sześć*, Warszawa 1910, p. 6.

regulation and statement of the law are noticed. The rights included in mind mean to the rights written down in a regulation the same as Plato's ideas mean to things. The rights existing for real are the same as Plato's things. According to Plato, the ideas exist separately from things, they create a separate world. According to Aristotle, they exist non-separately from things but as "the essence of these things embodying in them"[18]. One should state, agreeing with Plato[19], that the rights having their place in human mind exist separately from the rights which really exist— I do not agree with this opinion which consequently should be named as a radical conceptual realism[20]. One should add that inasmuch as Plato's things are cognized by senses and ideas by the mind, then the rights, both these existing in the world and these involved in mind and also these which are written down in a regulation, are cognized by the mind. One seemingly cognizes the rights by senses when he or she sees and hears the world around, when one reads or hears the content of regulations, however one sees the world, hears the sound, reads the signs but it is the mind which gives meaning to these signs and sounds. One should state in accordance with Aristotle, that the rights placed in mind exist non-separately from the rights written down in regulations, but they embody in them as the essence of those laws – the rights. I accept this view – a reasonable conceptual realism. This view is analogical[21] to conceptualism about which John of Salisbury writes[22].

I pay my attention that the rights which exist and which are included in the mind, as one understands them with the mind, find their description at two stages. At first, at the stage of creating the law, secondly at the stage of statement of the law. This phenomenon can be named as description of rights in the positive law.

6. The existence of rights

Using the arrangements of Plato, Aristotle and subsequent philosophers developing their concepts, one cannot run away from a certain question. Namely, where does the mind take knowledge about universals from and this question is turned for the benefit of my considerations into a question where does the mind take knowledge about rights from. There is a very well-aimed sentence of W. Tatarkiewicz which connects matters of mind with matters

[18] K. Twardowski, *O filozofii średniowiecznej…*, p. 40.
[19] For further details see: W. Tatarkiewicz, *Historia filozofii…*, p. 109.
[20] For further details, see: W. Tatarkiewicz, *Historia filozofii…*, p 317.
[21] I write this being aware of apparent contradiction of my thesis, in which I can see analogy between reasonable characters of realism and nominalism, however I do this with my eyes open, for the reason that I notice this analogy.
[22] W. Tatarkiewicz, *Historia filozofii…*, p. 322. K. Twardowski presents Abelard as the creator of conceptualism. (K. Twardowski, *O filozofii średniowiecznej…*, p. 53.), W. Tatarkiewicz disputes with this view but not with K. Twardowski (W. Tatarkiewicz, *Historia filozofii…*, p. 322)

of existence: “Anything which is given to senses and thinking — it is already a matter of existence”[23]. Thus, one can recognize that the rights included in mind belong to the existence. I do not think that the rights had only (in contrast to regulations) the nature of linguistic phenomena. The language describes meanings, however it does not create them. “The reality to which the words are related to” [24] builds the meaning of words. These words by L. Kołakowski rehearse a Socrates' view. On the other hand, L. Kołakowski writes about Parmenides: “(...) according to Parmenides, existence is indivisible, it has no levels of being, there is something or there is not, nothing intermediate. And existence is everything that it can be”[25]. The quoted sentences allow considering a human nature of right. If the right comes from a human establishment or from somewhere else. Where does the right come from? If the mind which involves the right creates it or just learns it. To continue further considerations, in particular according to Parmenides, I am forced to accept two assumptions. The first one — people are. The second one — the rights of these people exist as well. Hence people and their rights exist, then they belong to the existence[26]. Obviously, one more assumption has been made herein, namely that the existence exists. Therefore, one can notice that both people and their rights exist. They exist, so they belong to the existence. The existence is indivisible which results from the quote as well as that there are no levels of existence. If there are no levels of existence, then the rights exist to the same extent as people to whom rights are entitled to. Hence there are rights, it is not possible that they are not. The mind does not create rights, the mind only learns them. It does not seem that the rights occur apart from the world of people, that they fly like leaves in the air. Since that is not the way it is, then the rights are arguably related to people to whom they are entitled to. I am writing herein about a connection of rights with people and I am aware that I am making another assumption.

Coming back to Socrates, L. Kołakowski claims that he anticipates a Plato's theory of idea. This thesis, with which it is difficult not to agree, is very valuable to me as I indicate sources of legal conceptualism – the general theory of law in Peter's Abelard but also in Aristotle's and Aristotle leads forward to Plato. It is as much important for the theory being explained that the rights exist in the world and in mind, and regulations only describe them, concretise them. The rights are primary towards thoughts and towards words of regulations. The words of regulations relate to reality which builds the meaning of these regulations. The

[23] W. Tatarkiewicz, *Układ pojęć w filozofii Arystotelesa*, Warszawa 1978, p. 19.
[24] L. Kołakowski, *O co nas pytają…*, p. 8.
[25] L. Kołakowski, *O co nas pytają…*, p. 20.
[26] I pay the attention that the word "exist" appears herein in the existential sense, like at Parmenides'. (for further details: L. Kołakowski, *O co nas pytają…*, p. 16.)

reality I am writing about herein is a reality of rights. The existing rights and understood by mind. The reality of rights which are entitled to particular people but at the same time are strictly related to them. One can say that the rights and the people to whom they are entitled to are unity. The rights are not distinct from people. Hence, according to Parmenides' view, the existence has got no levels and simultaneously there is one existence, then a right and a human being to whom it is entitled to are the unity as they are the parts of the same existence. The presented considerations lead to a reflection that the rights are something like attributes particular people are characterized by. This thought corresponds to a Socrates' attitude according to which such concepts like justice or courage are not independent existences[27]. The rights are not these kinds of existences either. Just like height, sex or nationality are not separate existences but they only relate to a human being, they characterize him or her, the rights relate to a human being as well and characterize him or her. A man can be short, tall, pretty, ugly, young, old and a man still has got rights. The right is a human's attribute. The right is a human's attribute just like height, beauty, sex, age etc.

The most important thought of legal conceptualism (the general theory of law) is that the rights have got their place in the world and in human mind. This thought corresponds with Protagoras' of Abdera thought. The thought is as follows: "A human being is a measure of everything: everything that is, for the reason that it is and everything that is not, for the reason that it is not"[28]. The rights are strictly related to a man, however, the human mind concretises and specifies them. Hence the human mind concretises, specifies, discovers the rights, then the thought that a human being is a measure of rights seems to be well-aimed. In spite of the fact that a man and the right entitled to him or her are the unity, one cannot deny a role of mind in a process of establishing a content of right. The right exists but it is the mind, the wise human mind which establishes its content. The right exists but it is a man who by using the mind establishes that it exists. Thereby, the man is the measure of right. A man can be a measure of his or her own and someone else's right as well. If a man states that he or she has got a right to something, then he or she is a measure of his or her own right. A human being has got a right and understands it. If a man states that another man has got a right to something thereby he or she is a measure of right of this other person. A man states if a given right is entitled or not. The line of reasoning presented above is suitable to apply at probably all situations in which someone's right is being established. The judge who analyses a regulation and an actual state of affairs in which one should or not apply this regulation, is a measure of certain rights entitled

[27] L. Kołakowski, *O co nas pytają…*, p. 8.
[28] After: L. Kołakowski, Ułamki filozofii, Warszawa 2008, p. 6.

to certain people. The judge is a measure of these rights, in this certain situation of applying law. The judge analyses the regulation. The regulation has been created by a legislator. The legislator who formulates regulation is a measure of right from the abstractive point of view[29]. The legislator decides that in all actual states of affairs in which a regulation formulated by the legislator finds its application, the rights of people who contribute their actual states of affairs are shaping in a specific way — this way and not the other. The rights of possible participants of state of affairs are included in the legislator's mind, the legislator is their measure.

6.1. Rights as people's attributes

One should consider one more issue. It should be considered if a man is a measure of right for certain, a man who specifies and concretises this right or perhaps a measure of right is a man who is entitled to a right. I believe, as I has written previously, that a man to whom the right is entitled to is the unity with right, the right is his or her attribute just like height, skin colour or beauty. One looks at a man and sees if he or she is tall or short, if his or her skin is dark or light, if he or she is beautiful or ugly. Everyone who looks, makes such kind of assessments, declarations. One who looks uses his or her experience, his or her mind. The one is a measure who has got perception at his or her side[30]. The one who formulates an opinion is a measure. It is worth noticing that one can have perception of his or her own person and formulate an opinion about him or herself, however it does not change anything in the presented line of reasoning. Attributes of a person who one is looking at are invariable at a given moment. These attributes can be measured differently by different people. One can say about the same person that he or she is tall or short, pretty or ugly. Attributes do not change at a given moment. The existence lasts.

Likewise, the rights. I compare the right to an attribute of a certain person. The right is entitled to this person. This right is invariable at a given moment. It lasts. It lasts connectedly to a person to whom it is entitled to. Different people establish the existence or non-existence of this right, they consider its content. These people are measures of this right. Their minds specify and concretise the right. This process takes place in mind. The very right, as a person's attribute, is invariable at a given moment. Different subjects can assess them and concretise in many ways. It is worth asking a question if the presented view means relativism. Does a

[29] The truth is that the abstract measure of right is also a human being — a minister issuing a regulation, a president and members of Parliament establishing an act together.

[30] L. Kołakowski writes briefly but explicitly about knowledge, perception, legality of different human opinions, in a comment on Protagoras' sentence quoted in the main line of reasoning. L. Kołakowski. Ułamki filozofii. Warszawa 2008, p. 7.

statement claiming that a man is a measure of right with his mind threaten with breaking a principle of non-contradiction? It seems it does not. I have written above, that the rights are included in a wise mind. Thus, one should say that a wise man is a measure of right. A stupid man who does not use his or her mind can be compared to a false measure. This kind of man is like a false weight which is lighter than it should be.

7. Ontological proof for the existence of rights

A proof of Anselm of Canterbury, also known as Anselm of Aosta, and in religious tradition as Saint Anselm was supposed to prove the existence of a perfect person, even more perfect than the same existing one[31]. Gaunilo paid the attention[32] that both perfect persons, a more perfect one and a less perfect one, are in mind, thus it is not a proof at all. When the existence having its place in mind is sufficient, the existence in mind, then the proof analogical to Anselm's proof is sufficient.

8. A proposal of the theory's name – general theory of law

I notice a significant meaning of mind in views of John of Salisbury, Aristotle and even of Peter Abelard. The term: realism (legal) has got an established, distant from philosophical, meaning in the theory of law. On the other hand, the term: sermonism is proper only to the Abelard's attitude and sometimes it is unrecognizable even towards this approach. Thereby I postulate accepting the following name for my proposal: the conceptualistic theory of applicability and statement of the law and alternatively the legal conceptualism. The third name is used by myself the most frequently so far. This name is inspired, I do not conceal this fact, by a belief of Anaxagoras[33] who claimed that the mind was necessary to create the world. I add that it is necessary to create the statement of the law as well. The new name of theory is: the general theory of law. The name seems to be proper as the theory includes the natural and positive law and the statement and applicability of the law.

9. The addition to the H.L.A Hart's theory

I believe that there exist numerous different rights, each one separately. These rights are recognized in society — I agree with H.L.A. Hart at this point, however I consider the rule of

[31] W. Tatarkiewicz, *Historia filozofii*..., p. 305. I omit the content of proof by dint of the fact that it is generally known and by dint of saving space in the text.
[32] W. Tatarkiewicz, *Historia filozofii*..., p. 307.
[33] W. Tatarkiewicz, *Historia filozofii*..., p. 52.

recognition only as a method of recognizing rights. People recognize the applicability of law — I agree with H.L.A. Hart, however continuing considerations — I believe that people recognize the applicability of law as it refers to human rights which source is just the world and which understands and specifies human mind. The wise human mind involves the rights in itself. This mental coming the rights into being is primary or previous towards their recognition. If there were no rights and if the mind would not understand them, there would be nothing to recognize. H.L.A. Hart claims that the law obligates and simplifying — that the law is as people recognize that the law is. I ask, and I hope I answer the question: "why people recognize that the law is?".

10. Further possible direction of examinations

10.1. Authenticity of sentences of the law and legal sentences

When developing the presented theory one can do some research on the authenticity of a sentence of the law, the authenticity of legal sentence and possibility of proving these authenticities — I consider the way to do that in comparing the sentences of law and legal sentences to mental reality. It seems that the theory which I call the general theory of law allows examining if a sentence of the law is consistent to reality. Not to the reality cognizable empirically as it is rather a factor initiating creation of a sentence of law or it is its consequence. Thus, the empirical reality does not allow checking if the sentences of law are consistent to it. The sentences of law can be considered authentic if they refer to a reality that is distinct from empirical one. The reality different than empirical is recognized using the mind. Thereby, the sentences of law are authentic if they refer to the mental reality. If the sentences of law in this or other way describe rights and the rights which I present exist in mind, then the sentences of law are authentic. If the sentences of law do not refer to the authentic, existing in mind rights, they are unlawfulness dressed up in the clothes of law.

10.2. Variability vs. permanency of rights

Accepting the general theory of law as one's own view allows examining if the rights are permanent or if they change, both understand as a certain right of a certain human being and understood as a right comprehended generic, as the right entitled to a group of people or to all the people in the world. Thus, are they eternal and invariable or are they variable. It seems that they are invariable but only the subjects which recognize the rights and ways of recognition change.

10.3. The general theory of law as a common denominator

Development and in particular an accurate argumentation of legal conceptualism, should allow to treat it as a common denominator to other — previous theories of applicability of the law. As the legal conceptualism seems to be a common denominator, the name: general theory of law seems to be proper. I allow a possibility of considering the completion of positivism, normativism, natural law –religious and secular, using the proposed theory. The aim of this completion would be presumably the indication that the mentioned theories refer to the mind, to this what the mind understands, namely to the rights which exist. In this way my theory would become a common denominator to the mentioned above theories.

Part 2

Challenges of the Network and Digital Society

Chapter 1

CRIMINAL EVIDENCE IN THE NETWORK SOCIETY: NEW PROBLEMS, NEW SOLUTIONS?

Juhana Riekkinen

Researcher, University of Lapland, Faculty of Law, P.O. Box 122, FI-96101 Rovaniemi, Finland, juhana.riekkinen@ulapland.fi

Keywords: *Network society, criminal procedure, electronic evidence, cybercrime*

Abstract: *Novel problems relating to criminal evidence have emerged in connection with the recent developments of technology and society. In this paper, some of these legal and practical problems are identified and examined, with a distinction made between mostly cybercrime-specific problems and problems related to electronic evidence. This paper provides an overview of the topic and brings to light the need for continuing research in the field.*

1. Introduction

The rapid technological and societal developments that have taken us towards *the network society*[1] have transformed the context of criminal evidence. First, a new criminal phenomenon, often labelled *cybercrime*,[2] has emerged. It encompasses both wholly new kinds of crimes as well as computer-assisted versions of traditional crimes.[3] Second, the increasing pervasiveness

[1] For an overview of the concept as I use it, see J. van Dijk, *The Network Society*, London 2012.

[2] Largely interchangeable terms include computer crime, netcrime, Internet crime, e-Crime, and ICT crime. No commonly accepted definitions exist, and the exact demarcation of what constitutes a cybercrime and what does not is problematic. Nevertheless, there is a rather widespread consensus about the core meaning of the concept.

[3] The factor that the completely new crimes (e.g., computer break-ins and distributed denial-of-service attacks) and crimes applied to the network environment (e.g., distribution of child pornography on P2P networks, e-mail frauds, and hate speech or threats on websites) have in common is some sort of a connection to IT. At simplest, computer systems are usually either the instrument or the target of the crime. See, e.g., D. Brodowski, F.C. Freiling, *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft*, Berlin 2011, p. 28–29. See also U. Sieber, *Straftaten und Strafverfolgung im Internet*, München 2012, pp. 18–35, J. Clough, *Principles of Cybercrime*, Cambridge 2010, p. 9–10, C.L.T. Brown, *Computer Evidence: Collection and Preservation*, Boston 2009, p. 13, X. Li, *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*, Turku 2008, pp. 112, 132–146 and E.U. Savona, M. Mignone, *The Fox and the Hunters: How IC Technologies Change the Crime Race* [in:] *Crime and Technology: New Frontiers for Regulations, Law Enforcement and Research,* E.U. Savona (ed.), Dordrecht 2004, pp. 11–14.

of networks has affected the habits and operational patterns of criminals, who more and more use technological devices and networks for communication, preparations, research, planning, et cetera. As a result, *electronic evidence*[4] is often available even when the crime takes place in the physical world without any direct involvement of computers. Third, *police work and criminal investigations* have seen dramatic changes. On the one hand, old methods are insufficient in combatting and investigating new types of crime. On the other hand, new technologies have made it possible to collect various kinds of new evidence and analyse it in superior ways. Fourth, with the explosive increase in *surveillance and data mining*, potential electronic evidence is saved and stored in an ever-increasing quantity by private third parties and by security and intelligence agencies, even if such data is not primarily meant to be used as evidence. Fifth, *courtroom technology* and different applications of *e-Justice* are transforming trial procedures. Finally, *human and fundamental rights* have gained an increasingly important role, and must be taken into account in all areas of life and society.

All this suggests that the new network society has different demands for its law of evidence than the earlier, non-computerised and non-networked society. But does it require a wholly new approach to the law of evidence? Are the established rules and principles of procedural law flexible enough to adapt, or must they be replaced with new ones? If a new law of evidence is needed, what should it be like? Naturally, these questions cannot be answered exhaustively within the limits of this short paper. Instead, the aim of my paper is to map out some of the new, partially intertwining and overlapping problem fields related to criminal evidence in the environment of the network society.[5]

The following section briefly presents some characteristics of IT and networks that give rise to legal and practical problems. Subsequently, key problem fields are identified and examined, with a distinction made between problems mostly specific to cybercrime investigations, and those applying equally to all matters involving electronic evidence.[6]

---

[4] E. Casey, *Digital Evidence and Computer Crime*, Waltham 2011, p. 7, defines digital evidence "as any data stored or transmitted using a computer that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi." According to UNODC, *Comprehensive Study on Cybercrime*, New York 2013, p. 157, "Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form." The words digital and electronic are commonly used interchangeably. Cf. S. Mason, *Introduction* [in:] *International Electronic Evidence*, S. Mason (ed.), London 2008, pp. xxxv–xxxvi and B. Schafer, S. Mason, *The characteristics of electronic evidence in digital format* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012, pp. 23–30.

[5] By 'new' I refer to problems that have emerged and gained significance during the societal transition towards the network society—in other words, problems that were not relevant in the era before computer networks.

[6] Issues of electronic evidence are closely connected with cybercrime and frequently discussed together. In fact, by some definitions of cybercrime, the availability of electronic evidence makes the crime fall under the concept. See, e.g., I.M. Sunde, *IKT-kriminalitet: etterforskningsmetoder og personvern*, "Nordisk Tidsskrift for Kriminalvidenskab" 2000/3, p. 275 and J. Clough, *Principles of Cybercrime*, p. 10. With the current ubiquity of

Concurrently, some suggested and adapted countermeasures are described. The examination is deliberately confined to the operation of different national authorities: investigators, prosecutors, and judges.

2. Problematic characteristics of IT and networks

2.1. Structure of global networks

The most significant network of our time is, without a doubt, the Internet. Strictly speaking, the Internet is not a single network but a network of networks; an open-ended collection of interconnected computer networks of various sizes. It is not owned, centrally administered or controlled by any single party.[7] Without delving too deep into how the Internet functions from a technological viewpoint, each connected device, identified by an Internet Protocol (IP) address and sometimes an associated domain name, is connected to a network, which in turn is connected to other networks in a hierarchical fashion, all the way up to the so-called Internet backbone.[8] Data can be transmitted between any two devices on any two parts of the Internet. To achieve that, data is divided and encapsulated into small packets, which are routed through network adapters, switches, hubs, routers, and other network nodes until they reach their intended destination address, which is defined in the packet header.[9]

Vitally, the Internet is global and transnational. In the virtual world of networks, national borders are all but irrelevant. They do not—with some exceptions—hinder or block the movement of data,[10] which may travel instantaneously through dozens of countries as a result of a simple command given in one country. In the physical world, borders are still very much an obstacle for people, goods, and most importantly in this context, for national law, jurisdiction, and the operation of law enforcement authorities.[11] This difference between the virtual and physical worlds is a major source of legal and practical problems.

IT and surveillance, such a definition would expand the concept to cover almost all criminality, rendering it impractical and redundant.

[7] Specialised non-profit organisations such as the Internet Society and the Internet Corporation for Assigned Names and Numbers (ICANN) are involved in developing, governing and running the Internet, along with national governments, intergovernmental organisations, private network operators, and others.

[8] The so-called backbone is composed of multiple, largely redundant, high-speed optic fibre trunk lines that link large computer networks and core routers over great distances.

[9] See E. Casey, B. Turnbull, *Digital Evidence and…*, pp. 609–613 and U. Sieber, *Straftaten und Strafverfolgung…*, pp. 37–38.

[10] Various technical measures can be used to limit the availability of content based on location. Service providers may, e.g., make copyrighted content available only to IP addresses originating from a specified geographical region, and in several countries, measures such as IP address blocking, DNS filtering, and URL filtering are employed to censor Internet content. These measures can often be bypassed by skilled users.

[11] U. Sieber, *Straftaten und Strafverfolgung…*, pp. 35–36.

2.2. Pace of technological development

One of the fundamental characteristics of modern IT is its rapid development. Old technologies are being improved and replaced by new ones.[12] There are constant advances in processing speeds, storage capacities, connectivity, architecture and other properties, not to mention software and services. The range of IT devices is constantly broadening, and smart technology is making its way to places where it has not been utilised before. More and more of these devices are networked. In essence, IT and networks are briskly becoming ubiquitous.

The pace of development of computer and network technologies is linked to their highly generative nature, which has been attributed to their capacity for leverage across a range of tasks, adaptability to a range of different tasks, ease of mastery, and accessibility.[13] New hardware, software, and services are being developed by a mass of talented individuals, and by innovative companies with great resources. It is difficult for legislators, lawyers, prosecutors, and judges to keep up and to create, adapt, interpret, and apply the necessary legal rules.[14] This is not made easier by the fact that the legal world and lawyers tend to be rather conservative. As a result, both legal and practical problems arise.

2.3. High volumes of data and speed of network connections

The pace of development contributes to ever-increasing volumes of data in computer systems and networks, and to the speed with which information travels. Today, even an inexpensive consumer laptop or desktop computer possesses the capacity to store hundreds, if not thousands, of gigabytes of data.[15] The local storage capacity is augmented by many varieties of external and remote storage, including cloud services with servers scattered around the world. With the help of high-speed connections, data can be moved, copied, and deleted in an instant with little regard to geographical distances. The number of Internet users is estimated at more than 2.8 billion, the amount of connected devices is manifold, and the data traffic amounts to close to 2,000 petabytes per day. What is more, these figures are rapidly increasing.[16]

---

[12] Concerning technical obsolescence, see B. Schafer, S. Mason, *The characteristics of…*, pp. 31–32.
[13] J. Zittrain, *The Generative Internet*, "Harvard Law Review" Vol. 119, Issue 7, 2006, p. 1981.
[14] See U. Sieber, *Straftaten und Strafverfolgung…*, p. 39. It has been debated whether courts or legislatures are better capable of creating legal rules involving modern technology. See D.J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven 2011, pp. 165–167, in response to O.S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, "Michigan Law Review" Vol. 102, Issue 5, 2004, pp. 801–888.
[15] This is enough to store hundreds of thousands or even millions of photographs, or hundreds of hours of video.
[16] http://www.internetworldstats.com/stats.htm [29.9.2014] and http://www.cisco.com/go/vni [29.9.2014]. See also U. Sieber, *Straftaten und Strafverfolgung…*, pp. 38–39 and J. Clough, *Principles of Cybercrime*, pp. 5–7.

Consequently, the relevant data often plays the part of the needle hidden somewhere in a large number of haystacks of massive proportions; the huge volumes of data being processed, passing through networks, and stored on devices produce primarily technical and practical problems for investigators. These problems become legal in nature if they are circumvented with automated solutions and mass surveillance that compromise the rights of individuals, or conversely if they prevent the law enforcement from fulfilling their legal obligations to investigate crime. Moreover, when the amount of relevant electronic evidence identified by investigators is large, there may be further difficulties, delays, and costs in the trial phase, which in turn may jeopardise the procedural rights of the defendant (e.g., the right to fair trial).

2.4. Anonymity

Internet users can easily assume different identities, also false ones, in their online activities. The anonymity and impersonality of networks have been cited as a factor in enabling and encouraging different types of cybercrime, and in making online investigations difficult. In reality, however, online anonymity is often an illusion, as IP addresses can commonly be linked to persons, households or areas through subscriber information, logs and other data possessed by Internet service providers. Nevertheless, identification remains challenging, especially in cybercrime investigations involving determined and skilled perpetrators.[17]

On the other hand, online anonymity serves to protect individuals,[18] and it is closely connected with key human and fundamental rights of the network society, such as privacy and freedom of speech. In view of that, the powers granted to the authorities need to be balanced appropriately in order to minimise the negative impacts on the legitimate rights and interests of online users. Anonymity cannot be seen as just a practical hurdle in investigations.

3. Problems related to cybercrime investigations

3.1. Transnationality of cybercrime

The structure of the Internet allows data to cross national borders swiftly and frequently. It comes as no surprise, then, that cybercrime rarely remains within the borders of any nation state. Purely domestic cybercrime does exist,[19] but according to the national responses to the UNODC study, in the majority of countries 50–100 per cent of cybercrime acts encountered by

[17] See U. Sieber, *Straftaten und Strafverfolgung*…, pp. 36–37 and J. Clough, *Principles of Cybercrime*, pp. 6–7.
[18] Incidentally, also criminal investigators, as E. Casey, *Digital Evidence and*…, pp. 691–692, notes.
[19] This has been emphasised by X. Li, *Cybercrime and Deterrence*…, p. 152.

the police involve a transnational element.[20] If a cybercrime act ever comes to the attention of any police force,[21] the country in which the investigation is started may depend largely on chance. From early on, this transnationality has been widely acknowledged,[22] and international cooperation in the field has been pursued extensively. Several legal instruments have been created, the most significant and influential being the Council of Europe *Convention on Cybercrime* (2001). In these instruments, the focus has been on the harmonisation of material criminal law, jurisdiction, and international cooperation. Some provisions on procedural powers, electronic evidence, and the responsibility of service providers have also been included.[23]

Nonetheless, jurisdictional boundaries have not been erased. Gaps in *jurisdiction to adjudicate* have been reduced, but *jurisdiction to enforce* remains problematic. Even today, while data crosses borders easily, policemen do not. Most commonly, this problem has been tackled by improving the cooperation between authorities in different countries. Mechanisms for extradition of suspects are widely available, and as for evidence collection, mutual legal assistance procedures are commonly utilised.[24] Also informal cooperation between authorities exists.[25] As an alternative, national authorities could be granted the power to directly access extraterritorially stored data through a computer system within the national territory (*direct penetration/access*). While often faster and more useful in situations of urgency, this kind of power has been seen as violating the sovereignty of the target state, and is therefore available only in limited situations.[26]

It is worth noting that while problems of jurisdiction are highlighted in connection with the markedly transnational phenomenon of cybercrime, they apply to other transnational crime, as well. Consequently, the aforementioned solutions—international cooperation, mutual legal assistance, and direct penetration—concern any investigations where relevant electronic evidence is located extraterritorially.

---

[20] UNODC, *Comprehensive Study on…*, pp. 117–118, 183–184.
[21] The amount of undiscovered cybercrime (*Dunkelziffer*) is generally estimated as being very high.
[22] UNODC, *Comprehensive Study on…*, p. 5, cites a presentation at the Third INTERPOL Symposium on International Fraud, held in December 1979, as the earliest recognition of the "international dimension".
[23] For an overview of the most significant instruments, see UNODC, *Comprehensive Study on…*, pp. 63–72.
[24] These mechanisms, commonly based on bilateral agreements, are usually not specific to cybercrime or electronic evidence. See UNODC, *Comprehensive Study on…*, pp. 200–202.
[25] See UNODC, *Comprehensive Study on…*, pp. 210–214.
[26] See UNODC, *Comprehensive Study on…*, pp. 132–133, U. Sieber, *Straftaten und Strafverfolgung…*, pp. 77–80, D. Brodowski, F.C. Freiling, *Cyberkriminalität, Computerstrafrecht und…*, pp. 170–173, A. Pihlajamäki, *Tietojenkäsittelyrauhan rikosoikeudellinen suoja. Datarikoksia koskeva sääntely Suomen rikoslaissa,* Helsinki 2004, pp. 74, 84, 91, UN, *United Nations Manual on the prevention and control of computer-related crime*, 1994, paragraphs 261–267, and CoE, *Computer-Related Crime*, Strasbourg 1990, pp. 86–89. See also *Convention on Cybercrime*, Art. 32.

3.2. Lack of physical evidence and obscurity of the crime scene

The evidence of cybercrime acts is almost always in electronic form.[27] Eyewitness testimonies and traditional physical evidence are rarely available, and if so, they must first be located through online investigations. In contrast to traditional criminal investigations, electronic evidence is typically not just an additional element that can supplement other evidence, but an essential requirement for the success of the investigation and prosecution.

In traditional criminal investigations, the point of departure is usually the physical crime scene. Criminal acts in the physical world can often be linked to a single location where the act was committed, and perhaps to one or a limited number of other, adjacent locations in which the effects of the act can be observed. These locations can then be searched for weapons, tools, objects, fingerprints, footprints, blood, skin cells, and various other kinds of physical tracks, traces, prints, and marks that can be forensically analysed. In contrast, in the network environment, the perpetrator of the act typically uses a device in one place, anywhere in the world. As a result of a single click, data travels through various cables, routers, servers, and other devices, and brings about consequences in a wholly different location, or in a large number of locations, possibly distributed over a wide geographic area. The effects may even be observable from practically any device and location connected to the global network.

It is possible to conceptualise any computer or digital device linked to the crime as a digital crime scene, and valuable evidence can be located by searching them.[28] However, even in the fortunate situation that all of these digital crime scenes are located inside the jurisdiction in which the investigation is pursued, they may be difficult to find. Investigators may not be able to identify a natural starting place for their investigation, especially if they have no identifiable suspect. In this context, however, it should be noted that cybercrime is a wide concept that covers numerous dissimilar acts. For instance, a computer break-in typically has an identifiable target and victim. In such a case, digital traces are usually scattered along the path from the target device to the perpetrator's device. That path may be long and complicated, but at least one of the ends is known to the investigators. Following the cybertrail may, ultimately, lead to the suspect and produce useful evidence. In the case of distribution of copyrighted content through a P2P network, a different investigatory approach is required, as the copyright holders' locations are usually not relevant. Whether or not a clear physical starting location exists, information such as an IP address typically plays a major part in the early phases

[27] UNODC, *Comprehensive Study on…*, p. 122.
[28] For more about the similarities and differences of such digital crime scenes and physical crime scenes, see E. Casey, B. Schatz, *Digital Evidence and…*, pp. 190–192.

of the investigation. This heightens the importance of measures that allow investigators to receive subscriber information from ISPs or otherwise identify Internet users.[29]

3.3. Identifying and locating the suspect

If cybercrime takes place on the public Web, and if the perpetrator makes no effort in hiding their tracks, it is often relatively easy for the police, in cooperation with ISPs and website administrators,[30] to link the IP address to a person, household, or neighbourhood.[31] However, more dedicated cybercriminals have a wide range of tricks up their sleeve for masking their identity, including the use of free access points, encryption, proxies, onion routing, and anonymity networks such as Tor.[32] Much of the cybercriminal activity takes place hidden from the general public, on the Deep Web or the Darknet.[33] If a skilled perpetrator is determined to remain anonymous, tracking them becomes a task that requires high-level technical expertise and is still time-consuming at best, impossible at worst. If the perpetrator operates from abroad, the process may be further complicated. Obtaining the necessary information from foreign ISPs may be slow and difficult. A specified form or procedure, or the cooperation of foreign authorities, may be required.[34]

If a suspect can be identified, locating them is a matter of normal police work, made easier by the fact that the IP address can normally be linked to a physical address or location. In effect, it is frequently the location that serves as the basis of identification, as it is easier to locate the device used to commit the crime than to identify the perpetrator. IP addresses, subscriber records, and other such information are crucial for a successful cybercrime investigation, but are insufficient on their own: several people may have access to the same device, and criminals frequently commit crimes remotely by exploiting security vulnerabilities and taking control of

[29] See UNODC, *Comprehensive Study on…*, p. 143.
[30] About the interplay between investigators and private parties, see UNODC, *Comprehensive Study on…*, pp. 144–152.
[31] ISPs usually possess data with which the IP address can be linked to a subscriber. In some cases, a static IP address is assigned to a specific person. The use of dynamic IP addresses, which are automatically allocated to users for a limited period of time, complicates the process somewhat, because the investigators have to find out who the IP address was allocated to at the time of the act. Even this is usually possible as the ISPs maintain records of IP allocation. UNODC, *Comprehensive Study on…*, pp. 142–143 suggests that orders for subscriber information are the most commonly used investigatory power in cybercrime investigations.
[32] See U. Sieber, *Straftaten und Strafverfolgung…*, pp. 36–37.
[33] The Deep Web refers to the part of the Web that is not indexed by search engines. The Darknet refers to private, usually anonymous, distributed file sharing networks. J. Wood, *The Darknet: A Digital Copyright Revolution*, "Richmond Journal of Law and Technology" Vol. 16, Issue 4, 2010, pp. 16–19. Generally, see P. Biddle, P. England, M. Peinado, B. Willman, *The Darknet and the Future of Content Distribution* [in:] *Digital Rights Management*, J. Feigenbaum (ed.), Berlin/Heidelberg 2003, pp. 155–176. See also RCMP, *Cybercrime: An Overview of Issues and Incidents in Canada*, 2014, p. 13.
[34] About international requests for third parties, see UNODC, *Comprehensive Study on…*, pp. 149–150.

devices and network connections owned by others. Indeed, one of the greatest challenges from the prosecutorial point of view is the attribution of the acts committed through an identifiable *device* to a specific *person*, which often requires a combination of many types of evidence.[35] Thus, locating the device seldom marks the end of an investigation.

4. Problems related to electronic evidence

4.1. Obtaining data

Data connected with criminal activities can be gathered from numerous sources: the public Web, devices used by suspects and victims, and third parties that route, transmit, and control network traffic and data and offer online services. Multiple copies of the very same data may be stored on different platforms and in several locations, creating opportunities for investigators.[36] However, not all useful data is stored anywhere; transient data, which needs to be collected in real-time, may be highly valuable as evidence. Real-time collection may also be necessitated by reasons of urgency, or the volatility of stored data.[37]

Regardless of the source, the obtainment should be based on law. Investigators must have appropriate and effective, accurately defined investigative powers and coercive measures at their disposal. National legislative models on this matter, however, vary highly: In some jurisdictions, traditional, general provisions are applied and expanded to the new digital domain, whereas in others cyber-specific provisions have been created. The legal basis may also consist of a combination of the traditional, general provisions and the new, cyber-specific provisions, or the legal powers may be altogether insufficient or insufficiently regulated.[38]

As a general rule, coercive measures are not needed when data is gathered from victims with their consent or from the public Web, and few legal concerns have been raised in relation to this kind of evidence collection.[39] When it comes to devices associated with suspects, above all, the powers of search and seizure come to play. When such a device is found, a 'bit-for-bit'

---

[35] UNODC, *Comprehensive Study on…*, p. 169. The attribution problem applies to electronic evidence of traditional crime, as well. See E. Casey, *Reconstructing Digital Evidence* [in:] *Crime Reconstruction*, W.J. Chisum, B.E. Turvey, Burlington 2006, pp. 431–433.

[36] B. Schafer, S. Mason, *The characteristics of…*, p. 49, see also pp. 33–35.

[37] UNODC, *Comprehensive Study on…*, p. 130.

[38] See UNODC, *Comprehensive Study on…*, pp. 122–126. In the US, for example, the more than 200-year-old Fourth Amendment, which sets limits on searches and seizures, is applied to modern digital searches along with newer, specific provisions. See O.S. Kerr, *Searches and Seizures in a Digital World*, "Harvard Law Review" Vol. 119, Issue 2, 2005, pp. 531–585 and O.S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, "Stanford Law Review" Vol. 62, Issue 4, 2010, pp. 1005–1049.

[39] However, from the national perspective, legal issues may be raised by covert police operations and agent provocateur activities on the public Web. See U. Sieber, *Straftaten und Strafverfolgung…*, pp. 125–126. From the international law perspective, see U. Sieber, *Straftaten und Strafverfolgung…*, pp. 77–80 and D. Brodowski, F.C. Freiling, *Cyberkriminalität, Computerstrafrecht und…*, p. 170.

copy of the entire storage media is often created for investigatory purposes, but in some cases the seizure may also be limited to some identifiable data.[40] In addition to searches and seizures of stored computer data, different forms of real-time data interception, collection and remote surveillance may be used to gather evidence, usually covertly. These may involve the cooperation of service providers or the use of remote forensic tools.[41]

When relevant data is in the possession of third parties, searches and seizures are mostly unfeasible due to the interests of the third parties and the high volumes of cases and data. Instead, authorities should be allowed to order the expedited preservation or "quick freeze" of volatile or temporary data, and then later, if needed, the production of that data.[42] In the provisions concerning such orders, legal distinctions are often made between different categories of data, such as subscriber data, traffic data, and content data.[43] In practice, various service providers hold plenty of such data for their internal purposes,[44] and they have also been given legal obligations to retain, typically for a defined period of time, certain types of data that may be useful for purposes of law enforcement.[45] Furthermore, third parties may otherwise cooperate with criminal investigators and other authorities, willingly or unwillingly.[46]

The impact and intrusiveness of the powers described above varies. For instance, preservation orders generally represent a much smaller privacy threat to individuals than real-time surveillance of all of their online behaviour.[47] Taking this into consideration, each power must be balanced with proportionate procedural safeguards. These typically include the definition of conditions and circumstances for usage, time limits, and prosecutorial or judicial oversight.[48] Non-compliance with these legal provisions may, among other consequences, lead to challenges against the admissibility or reliability of the gathered data in the subsequent trial.

---

[40] The limitation of copied material may be less intrusive, but it is generally inadvisable to just turn on the computer and start browsing through files and folders in search for the relevant data. This may result in the loss of valuable evidence, and the integrity, authenticity, and completeness of the data may be challenged by the defence. See C.L.T. Brown, *Computer Evidence: Collection…*, p. 268 and E. Casey, *Reconstructing Digital Evidence*, p. 425.

[41] The tools used by the authorities very much resemble those used by cybercriminals, including spyware, Trojans, key-loggers, and remote-administration software. Such tools are sometimes called *policeware* or *govware*.

[42] See UNODC, *Comprehensive Study on…*, pp. 126–128.

[43] UNODC, *Comprehensive Study on…*, pp. 129–130.

[44] See UNODC, *Comprehensive Study on…*, pp. 144–148.

[45] The legal validity of mass data retention obligations has been called into question. Notably, the European Court of Justice declared the EU Data Retention Directive (2006/24/EC) to be invalid (C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others*, 8.4.2014). In the wake of the judgment, the legality and constitutionality of national implementations of the directive have been debated and challenged in national courts.

[46] Especially problematic is the cooperation with other security and intelligence agencies (e.g., the NSA) in the realisation of surveillance measures. Particularly when surveillance is exercised indiscriminately without connection to a specific target, suspect or criminal act, it is often highly problematic from the legal point of view.

[47] The harms of online surveillance can largely be likened to those of continuous electronic video surveillance, aptly described by D.J. Solove, *Nothing to Hide...*, pp. 178–180. The privacy risks may be even greater, because online behaviour is often more private and intimate in nature than behaviour in physical public spaces.

[48] For an overview of existing national safeguards, see UNODC, *Comprehensive Study on…*, pp. 135–138.

The global nature of networks frequently complicates the obtainment of data. Tracing and locating relevant data may prove challenging for investigators, and their legal powers may run into national boundaries. Even if data is accessible, its physical location may be undeterminable due to the *loss of location*[49] connected with cloud services, causing problems of jurisdiction.[50] In addition, investigators are met with several technical and practical challenges in obtaining electronic evidence. First, the high volumes of data and varied ways of storage make searches and other kinds of measures, as well as subsequent examination and analysis, time-consuming and expensive.[51] Second, the use of passwords, encryption, dead man's switches[52], and other anti-computer forensics measures employed by those who want to keep their possibly incriminating data inaccessible further complicates the extraction.[53] The use of inappropriate forensic methods or tools may result not only in failure to obtain the data, but also in the loss of the data. Third, forensic failures and inadequate documentation of the extraction procedure may diminish the reliability and evidentiary value of the obtained data, and result in unsuccessful prosecution.[54] For these reasons, manuals and guidelines have been written, and a lot of thought has been given to the training of first responders, digital forensics specialists, and prosecutors.[55] Of course, constant technological development makes it challenging for organisations and personnel to maintain the necessary level of expertise and skills.

4.2. Preservation and storage of data

Once obtained, the data must be preserved and stored for further actions, and the authenticity, integrity, and completeness of the data must remain guaranteed at all stages from

---

[49] See J. Spoenle, *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Strasbourg 2010, pp. 5–6 and B. Schafer, S. Mason, *The characteristics of...*, pp. 34–35.

[50] On the other hand, users of online services—especially cloud services—are often unaware of the physical location of their data. They may not know which measures they may be subjected to, which safeguards are applied, and which remedies are available. There may be conflicts of laws or jurisdictional gaps. See UNODC, *Comprehensive Study on...*, pp. 140–141.

[51] U. Sieber, *Straftaten und Strafverfolgung...*, p. 39 and B. Schafer, S. Mason, *The characteristics of...*, p. 49.

[52] A dead man's switch refers to a script or other software that reacts in some automated fashion to a specific triggering event, such as the loss of network connection. It could be used by criminals to delete traces of evidence upon detection, or danger thereof. C.L.T. Brown, *Computer Evidence: Collection...*, pp. 54, 68.

[53] E. Casey, *Digital Evidence and...*, p. 458, describes password protection and encryption as two of the greatest obstacles that investigators face today. About encryption, see S. Mason, *Encrypted data* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012, pp. 193–216. About anti-forensics measures in general, see B. Schafer, S. Mason, *The characteristics of...*, pp. 53–68.

[54] G.R.S. Weir, S. Mason, *The sources of digital evidence* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012, p. 9.

[55] For example, the United States Department of Justice has been active in this matter. See USDOJ, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*, 2007 and USDOJ, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement*, 2004. For a list of various guidelines, see S. Mason, A. Sheldon, *Proof: the investigation, collection and examination of digital evidence* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012, pp. 73–74.

the seizure or other obtainment until the trial and beyond. The police and the prosecution need to be able to demonstrate the continuity of the electronic evidence by maintaining a documented chain-of-custody for both the physical device and the data. As data can be altered easily, a failure in this respect may leave the electronic evidence susceptible to being challenged in the court.[56] The requirements for the preservation are, in essence, determined by the legal norms on the admissibility and evaluation of evidence, and the burden of proof required in the trial. The methods as such are seldom defined in legislation. In practice, the authenticity and integrity of data are commonly guaranteed with cryptographic hashing, checksums, and documentation.[57] To avoid loss or corruption of data, forensic operations are ordinarily performed on copies.[58]

Additionally, data storage may present practical difficulties. Storage capacity in itself is inexpensive today, but for criminal evidence, the requirements for capacity and reliability are extremely high. Authorities may need to invest considerably in data security, technical measures for keeping back-ups and duplicates, and even climate-controlled storage facilities.[59]

4.3. Presentation, admissibility, and evaluation of data

So far, little has been done to harmonise the presentation, admissibility, and evaluation of electronic evidence internationally.[60] In some countries, specific legislation concerning electronic evidence has been introduced, while in others, existing concepts, rules, and principles have been applied analogously, and in yet others, a combination of these strategies has been utilised.[61] In the civil law tradition, emphasis has been placed on the free theory of evidence, which includes the principles of free introduction and free evaluation of evidence. As a result, most of the civil law countries—and many others—place no or minimal conditions on the admissibility of electronic evidence, do not regulate the means of its presentation, and leave its evaluation to the free discretion of the judge. The presentation and evaluation of electronic

[56] UNODC, *Comprehensive Study on…*, p. 158, S. Mason, A. Sheldon, *Proof: the investigation…*, p. 88, and E. Casey, *Digital Evidence and…*, pp. 21–24, 59–60.
[57] S. Mason, A. Sheldon, *Proof: the investigation…*, p. 87, E. Casey, *Digital Evidence and…*, p. 20, and C.L.T. Brown, *Computer Evidence: Collection…*, pp. 8, 235–238.
[58] UNODC, *Comprehensive Study on…*, pp. 159–160, E. Casey, *Digital Evidence and…*, p. 26, and E. Casey, *Reconstructing Digital Evidence*, pp. 425–426.
[59] UNODC, *Comprehensive Study on…*, pp. 164–165, 169 and S. Mason, A. Sheldon, *Proof: The Investigation…*, p. 89.
[60] As an exception, see CoE, *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology*, paragraph 13.
[61] B. Schafer, S. Mason, *The characteristics of…*, p. 23.

evidence have been seen as bringing about only limited legal problems, if any.[62] In contrast, in the common law tradition—characterised by oral, highly adversarial jury trials—the admissibility of digital data has been debated, for instance, in relation to the different rules of evidence (e.g., the best evidence rule, the hearsay rule, and the various exclusionary rules).[63]

In all legal systems, some human-comprehensible means and manner of presentation is required in trial, as even the most tech-savvy judge or jury can hardly draw conclusions from a string of bits.[64] Many practical questions need to be answered: For example, should electronic evidence be presented directly through digital devices, or as paper printouts? Which evidence presentation systems, hardware, and software should be used? When should the data itself be presented, and to what extent should expert and police testimonies, reports, explanations and visualisations be relied upon? In the absence of legal norms, these choices often fall to the discretion of prosecutors or judges. Currently, the answers may be sought on a case-by-case basis, or even be determined by random circumstances, such as the availability or unavailability of a certain piece of equipment in the courtroom.[65] This is unsatisfactory, as the presentation may affect how the evidence is interpreted and evaluated.[66] Adoption of best practices, guidelines, or specific legislation could diminish the time spent on repeatedly having to solve the same problems, and contribute to a more unified and predictable practice.[67]

A major concern regarding evaluation is whether judges and juries possess enough basic technological understanding to correctly determine the meaning, weight and trustworthiness of a particular piece of electronic evidence. Expert statements and testimonies are no doubt crucial, but the triers of fact themselves certainly need to be IT literate. As electronic evidence becomes ever more significant, even in cases of traditional crime, the educational challenge is not limited

---

[62] U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, 1998, p. 126 and A. Pihlajamäki, *Tietojenkäsittelyrauhan rikosoikeudellinen suoja…*, p. 73. About admissibility concerns in the US, see E. Casey, *Digital Evidence and…*, pp. 56–68. See also UNODC, *Comprehensive Study on…*, pp. 55, 158.

[63] U. Sieber, *Legal Aspects of…*, pp. 127–129. See also UNODC, *Comprehensive Study on…*, p. 55, 158. In many civil law countries, evidence (including digital data) may nowadays be excluded if it has been obtained illegally, or if its use would violate the human and fundamental rights of the defendant. In part, this is due to the recent case law of the European Court of Human Rights. However, some civil law countries, for example Germany, have had a tradition of exclusionary rules that predates this.

[64] In fact, electronic evidence is *always* dependent on machinery and software—not even the 0's and 1's on a storage medium can be observed with the naked eye. See B. Schafer, S. Mason, *The characteristics of…*, p. 30.

[65] Of the different means currently employed, see UNODC, *Comprehensive Study on…*, p. 167.

[66] See, e.g., D. Schofield, S. Mason, *Using graphical technology to present evidence* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012, pp. 221–224. The use of computer-generated visualisations, animations, simulations, virtual reality applications, etc., is an interesting topic in its own right, and its pros and cons have been discussed in connection with the debate on the competency of juries. See E.C. Wiggins, *What We Know and What We Need to Know About the Effects of Courtroom Technology*, "William & Mary Bill of Rights Journal" Vol. 12, Issue 3, 2004, pp. 739–742.

[67] Best practices have been suggested by, e.g., U. Sieber, *Straftaten und Strafverfolgung…*, p. 127. About presentation from an investigator's point of view, see E. Casey, *Digital Evidence and…*, pp. 75–81.

to law enforcement and prosecution, or to specialised judges, but applies to the judiciary as a whole.[68] At times, this has not been adequately recognised.[69]

5. Concluding remarks

In this paper, I have mapped out some of the problems that the law of evidence faces in the network society. A good deal of research in the field has already been carried out, but continuing research is needed to keep up with the constant developments, to specify the problems in more detail and more comprehensively, and to determine the suitability of the few described solutions on both international and national levels, as well as to craft new solutions. The same need applies to the perspectives deliberately left out of this paper, such as the possibilities of private parties to obtain and present electronic evidence on their own.[70]

Although I have focused on problems, technological developments also afford solutions to old predicaments and generate entirely new possibilities. In the network society, legal scholars, lawyers, and legislators should not be locked into thinking conservatively about the difficulties that new technology causes. It is essential to embrace, while paying due respect to the rights of the individual, new technological advances and prospects. Besides, law not only needs to react to positive and negative developments; it should also be used as a proactive instrument to encourage and promote innovation and progress. To sum up, I feel that lawyers could take an example from the positive attitude towards technology commonly found in professional groups such as IT specialists, engineers, and law enforcement personnel—and even criminals.

[68] Similarly, UNODC, *Comprehensive Study on…*, p. 172.
[69] For example, *Finland's Cyber Security Strategy*, Helsinki 2013, p. 7, stresses the importance of making certain that the police have sufficient capabilities to prevent, expose and solve cybercrime, but makes no mention of the role of prosecutors and judges. The Strategy's *Background dossier*, Helsinki 2013, p. 13, however, states summarily that "The competence of the authorities, prosecutors and judges involved in the prevention and investigation of cybercrime is improved by developing the pertinent education of the field."
[70] Various related topics that are not addressed here include: electronic hearings, electronic filing and management of cases and evidence, legal AI, and many other aspects of courtroom technology and e-Justice.

Chapter 2

STILL HIGH IN THE SKY: FACING LEGAL CHALLENGES OF CLOUD COMPUTING IN THE EU

Agata Jurkowska-Gomulka

Professor, Chair of Administrative Law, University of Information Technology and Management, Sucharskiego 2, 35-225 Rzeszow, Poland, ajurkowska@wsiz.rzeszow.pl

Keywords: *cloud computing; data protection; data security; European Cloud Computing Strategy; soft law*

Abstract*: Cloud computing is not a particular information technology but a concept/channel of communications, sometimes compared to network services such as providing gas or electricity. Cloud computing, giving an opportunity to use IT infrastructure and tools as a service, not a product, has become one of the most influential tendency in a development of modern IT, being a popular method of outsourcing of IT services for companies and individuals.*

A paper identifies key regulatory problems presently faced by cloud computing. Then a paper delivers a general overview of existing EU legal provisions that can be applied to cloud computing. The application of current regulations to solving problems resulting from cloud computing is rather limited what was confirmed by an opinion on data protection in cloud computing announced in July 2012 by so called Article 29 Working Party. The further part of a paper brings the analysis of the Commission's initiatives concerning cloud computing. Commission's strategy on cloud computing seeks solutions of many issues related to cloud computing in future (currently under preparation) EU regulations such as so-called General Data Protection Regulation and others.

The paper concludes that the EU's regulatory policy on cloud computing should be based on 'soft framework' (unbinding soft law and policy measures) rather than binding regulation.

1. Cloud computing - key technical and economic facts

Cloud computing is not a particular information technology but a concept/channel of communications, sometimes compared to network services such as providing gas or electricity. Cloud computing gives an opportunity to use IT infrastructure and tools as a service, not a product. Cloud computing has become one of the most influential tendency in a development of modern IT, being a popular method of outsourcing of IT services for companies and individuals. Cloud computing is considered 'the most pervasive delivery method for IT services'[1], 'a global technological paradigm'[2], 'one of the biggest technological revolutions to emerge in recent times'[3]. People commonly use cloud computing even without awareness that they are doing so: what, if not cloud computing, YouTube is?

The first use of a term cloud computing is assigned to Prof. Kenneth K. Chellapa who used it in 1997 to say that *'a computing paradigm where the boundaries of computing will be determined by economic rationale rather than technical limits'*[4].

Cloud computing is a very broad term, without unique definition, covering differentiated types of clouds and business/infrastructure models. One can identify public or private clouds. The first is dedicated to an individual organization (company, institution), it may be located at organization's premises or its management can be outsourced. Usually a private cloud remains under a total control of a cloud user. A public cloud is owned and managed by a provider that supplies services to private users, business and administrative bodies. Services in a public cloud are usually accessed via the Internet. In a public cloud a provider holds a key role as, regarding a character of this business model, a cloud user transfers its control over data to cloud provider. Therefore, a majority of problems identified as 'legal challenges' of cloud computing occur in a functioning of public clouds. These challenges may also arise in 'community' or 'hybrid' clouds that - as their names suggest - combine elements of private and public clouds.

There are three models of provision of cloud computing services, applied in all types of clouds. IaaS (Cloud Infrastructure as a Service) is a model where a cloud provider leases

---

[1] *Report on Cloud Computing and the Law for UK FE and HE - An Overview*, JISC Legal information, 31.8.2011 (available at: http://www.jisclegal.ac.uk/ManageContent/ViewDetail/ID/2137/Report-on-Cloud-Computing-and-the-Law-for-UK-FE-and-HE--An-Overview-31082011.aspx, visited 6.3.2015; hereafter, JISC Report).

[2] Opinion 05/2012 on Cloud Computing, Article 29 Data Protection Working Party (available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf, visited 6.3.2015), p. 2 (hereafter, Art. 29 Working Party Opinion).

[3] Art. 29 Working Party Opinion, p. 4.

[4] R.L. Kachur, W.J. Kleinsmith, *The Evolution to the Cloud – Are Process Theory Approaches for ERP Implementation Lifecycles Still Valid?*, "Business Systems Review" 2013/3, p. 76-77; M. Pérez-Cota, R. Gonçalves, F. Moreira, *Cloud Computing Decisions in Real Enterprises*, [in:] *Agile Estimation Techniques and Innovative Approaches to Software Process Improvement* (R. Colomo-Palacios and others ed.), IGI Global, 2014, p. 313.

technological infrastructure. In SaaS (Cloud Software as a Service) a provider can supply various application services; in this model users are provided with business-specific capabilities, such as e-mail or customer management. PaaS (Cloud Platform as a Service) is a model where a provider delivers advanced development and hosting of applications, it allows organizations and developers to extend their IT infrastructure on-demand basis[5].

A list of advantages of cloud computing is almost never-ending, but among them the first place are taken by: availability of a certain content always and everywhere, through various appliances (desktop computers, laptops, smartphones, tablets, etc.), easiness in modifying contents (new items can be added very quickly and they can be available at one), relatively low costs of cloud computing services (paying only for usage, avoiding fixed costs).

European Commission considers cloud computing as an instrument for enhancing productivity of the European economy. Each organisation is able to reduce its costs by 10-20% on average while applying cloud computing. is estimated that cloud computing will have a cumulative impact on EU's GDP of EUR 957 billion by 2020 and in the same period it will create up to 3.8 million jobs[6]. Economic benefits of cloud computing are commonly recognized worldwide, not only in the EU[7].

2. Cloud computing - key legal problems

A number of legal problems related to cloud computing seems to be as big as a number of varieties of models for providing this type of IT services. Cloud computing is based on outsourcing which as such creates many legal doubts, mainly concerning legal liability towards clients and contractors. A list of legal controversies accompanying cloud computing is quite long, the most common issues mentioned in this context are: data protection, confidentiality, jurisdiction, freedom of information, copyright, even equality legislation sometimes appear[8]. In total they all sound like a list of wishes of a dream-client of every legal company. A serious legal literature on cloud computing is rather modest but one can extremely easily find practicing lawyers' guidelines on cloud computing problems.

---

[5] P. Mell, T. Grance, *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology Gaithersburg, September 2011.

[6] Data presented in: G. Cattaneo, M. Kolding, D. Bradshaw, G. Folco, IDC, *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up*, SMART 2011/0045, D2-Interim Report, 24 February 2012 (available at http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf, visited 6.3.2015).

[7] See one of the most recent summary of economic benefits predicted by various policy centres: R. Samani, B. Honan, J. Reavis, *CSA Guide to Cloud Computing. Implementing cloud privacy and security*, Syngress 2015, p. 9-13.

[8] See e,g, JISC Report, p. 5.

In general, legal problems associated to cloud computing can be categorized, at least due to a criterion of entities touched by particular problem, in two groups: problems regarding relations between cloud provider and cloud user (issues that are covered by private law) and problems concerning a legal and factual situation of external entities, not engaged in a cloud provider - cloud user relation (issues covered either by private or public law). The first category makes a home for such problems as ownership of the data, data location and transfer or data preservation after termination of a contract. The second category covers problems of 'external' entities whose data should be protected within a flow of services between a cloud provider and a cloud user - these problems can be also called secondary because they always result from problems that occurred in relations of a provider and a user. Potentially unlimited scope of victims when a security of data stored by a cloud supplier is endangered makes in opinion a question of data protection absolutely the hottest legal challenge of cloud computing.

The most 'vivid' problems of cloud computing can be also categorized, due to a criterion of a value that need protecting, as security problems and ownership problems, the latter including copyrights. Surely, a response to all problems, no matter what value is touched, is just formulating an adequate scope of liability of a particular member of a system (cloud supplier, cloud user).

Regarding a data protection the biggest problem is a lack of control over personal data as well as insufficient information with regard to how, where and by whom the data is being processed or/and sub-processed[9]. This uncertainty on many (or even a majority) aspects of data portability may dispose cloud users, and also persons whose data are just stored, of a possibility of a proper protection of their rights of various kinds, mainly right to privacy, but also copyright.

What was not caught by categorizations presented above are also specific legal challenges of cloud computing for a public sector[10].

But what was described above as legal problems of cloud computing constitutes only one level of legal challenges that can be considered as detailed and 'personalized'. The second (or rather *meta level*) of legal challenges is a choice of legal system that should (or even: must?) be applied in order to solve particular problems[11]. Unfortunately, World Wide Web totally ignores

[9] Art. 29 Working Party Opinion, p. 5-6.

[10] The issue is developed in an interesting report prepared by L. Hellemans for Cloud for Europe on legal aspects of Cloud Services in the European public sector and legal project support (document described as D2.1. Legal implications on cloud computing, 1.5.2014; available at http://www.cloudforeurope.eu/documents/10179/15444/D2.1+Legal+implications+on+cloud+computing+v1/023da045-4c78-4cd7-afe6-0a5de01c0347, visited 6.3.2015).

[11] This problem is developed by F. Fangfei Wang, *Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction*, "European Business Law Review" 2013/5, p. 589–616.

territorial boundaries of legal systems so it is not easy to guess law of which country should be applied. In the EU the most controversial issues in cloud computing (ones related to data protection) are regulated (assuming that 'traditional' regulations can be applied to cloud computing) by directives so legal systems in Member States usually differ. But it is not only a case of diverging legislations intra EU, it is also a problem of escaping to legal systems outside the EU whose regulation, specially of data protection, is considered as very restrictive and non-compliant with current requirements of technological development.

3. Down on the Earth - legislation being applied to cloud computing

When basic legal problems of cloud computing are identified it is possible to find regulations in force that can be applied while waiting for (if any) specialised legislation on clouds. A presentation below concerns only, although existing or prospect, EU law as it puts limits to national laws. At the very beginning it must be underlined that in a situation of a lack of EU's legislation on cloud computing so in solving legal issues more 'general' instruments and acts must be used (and 'general' here is meant also as a legal act concerning information technologies, but not necessarily cloud computing).

In the proposed pattern data protection, regarded as a central problematic point of cloud computing, is subject to EU Data Protection Directive (95/46/EC)[12] and the E-privacy Directive (2002/58/EC[13] as revised by 2009/136/EC[14]). The latter can be applied to cloud computing only if a cloud provider acts as providers of a publicly-available electronic communication service.

A cloud user (cloud client) can be regarded as a 'controller' in the meaning of Art. 2d and a cloud provider as a 'processor' in the meaning of Art. 2d Directive 95/46/EC. The principle of purpose specification and limitation of data (personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes), expressed in Art. 6(b) Directive 95/46/EC, should be applied to data collected in clouds. The same applies to the principle of erasure of data (Art. 6e). In the light of a Directive a burden of securing data lies on cloud providers - they are obliged to guarantee a confidentiality

[12] 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, OJ L 281, 23.11.1995, p. 31–50.
[13] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.7.2002, p. 37–47.
[14] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11–36.

of data and for adopting all security measures that are prescribed in controller's and processor's national laws based on the EU standards. It is also cloud client's responsibility to choose a cloud provider that is able to achieve all goals of data protection (not only the classical triangle: availability, confidentiality and integrity, but also: isolation, intervening, accountability and portability) in compliance with EU rules (Art. 17(2) Directive 95/46/EC). Subcontracting of data processing must be reported by a cloud provider to a cloud client, however, there are still doubts if a controller's (cloud client's) consent is necessary for setting subcontractors up. Due to Directive 95/46/EC this is a cloud user that provides a data subject from whom data relating to himself are collected with information on his identity and the purpose of the processing[15].

Directive 95/46/EC allows for an (even doubtful) determining a law that should be applied to a controller of a data (this is cloud user) with one or more establishments within the EEA and also to the law applying to controllers who are outside the EEA but use equipment located within the EEA to process personal data. According to Art. 4.1.a. Directive 95/46/EC the law of a country where a cloud user is established should be applied (as a basic solution). Consequently, if a cloud user is set up in more than one Member State laws of each of these countries should be applied. Moreover, EU law has still its power when a cloud user is established outside the EEA but it uses any (automatic or non-automatic) equipment in any Member State (in some countries equipment means also browse cookies), unless this equipment is used only for a transit of data (Art. 4.1.c)[16].

Article 25 and 26 of the Directive 95/46/EC provide for free flow of personal data to countries located outside the EEA only if that country or the recipient provides an adequate level of data protection, otherwise specific safeguards must be put in place by the controller and its co-controllers and/or processors). Art. 29 Group correctly points in its Opinion that regarding a characteristic features of clouds which is 'complete lack of any stable location of data within a network, ' cloud client is therefore rarely in a position to be able to know in real time where the data are located or stored or transferred'[17]. As a consequence, this is a typical 'mission impossible' to identify legal standards that should be applied in terms of data protection when data are transferred to non-EU countries. On the other hand, if a model clauses

[15] C. Van Alsenoy, *Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC*, "Computer Law and Security Review" 2012/1, p. 25-43.
[16] W. Kuan Hon, J. Hörnle, Ch. Millard, *Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing*, "International Review of Law, Computers & Technology" 2012/2-3, p. 129-164.
[17] Art. 29 Working Party Opinion, p. 17.

2010/87/EC can be applied in case of a data transfer outside the EU, it is rather doubtful if it can be applied to intra EU contracts.

Opinion of Art. 29 Working Group can be considered as very helpful in interpreting Directive 95/46/EC for entities already engaged or planning to get engaged in contracts on cloud computing. However, it is nothing more but a guideline, it is not even a soft law, although the Group sees it as 'sound basis for securing the processing of personal data that EEA-based clients submit to cloud providers'[18].

A scope of legislation as well as a usefulness of existing EU regulations for governing cloud computing is rather modest[19]. As P. Van Eecke correctly claims: 'cloud computing is all about reducing the level of direct control, while EU legislation is all about keeping control of data'[20]. It leads us to inevitable questions: can cloud computing be subject to any regulations at all? Is the EU in a position to regulate such an undefined and rapidly changing phenomenon?

4. High in the sky - legislation that could be applied to cloud computing

The starting point for discussing a future of legislation on cloud computing is a claim that: there is a rapid growth of cloud computing that create many specific legal problems and an existing regulation does not meet all (if any) legal challenges of cloud computing. The EU is attempting to meet these challenges in a complex manner as it is presented in the Commission's strategy on cloud computing that took a form of a communication (adopted on 27 September 2012) addressed to European institutions, titled 'Unleashing the Potential of Cloud Computing in Europe'[21] (hereafter, CC Strategy). The CC Strategy aims at 'enabling and facilitating faster adoption of cloud computing throughout all sectors of the economy which can cut ICT costs (...)'[22], in order to boost productivity, growth and jobs. It constitutes a part of Digital Agenda (Digital Single Market) - a broader concept of the Commission's policy in new

[18] Art. 29 Working Party Opinion, p. 22.
[19] See e.g. S.Y. Esayas, *A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data*, "Computer Law and Security Review" 2012/6, p. 662-678.
[20] P. Van Eecke, *Cloud Computing. Legal issues* (available at http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf, visited 6.3.2015).
[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Unleashing the Potential of Cloud Computing in Europe, Brussels, 27.9.2012 COM(2012) 529 final (hereafter, CC Strategy).
[22] CC Strategy, para. 1, p. 2.

technologies. The Commission also tries to combine European Cloud Computing Strategy with a European Strategy on Cyber Security[23].

The CC Strategy focuses on three fields (actions): cloud standardisation ('Cutting through the Jungle of Standards'), pure legal issues ('Safe and Fair Contract Terms and Conditions'), institutional cooperation, governance and consultancy ('European Cloud Partnership').

Standards necessary in cloud computing concern security, interoperability, data reversibility and portability. Standardisation as Key Action 1 of the European Cloud Computing Strategy aims at creating - as the Commission calls it - 'cloud-friendly' Europe. It requires building confidence of all stakeholders, including private users in cloud computing, especially because their position *vis-a-vis* cloud suppliers is relatively weak. But standardisation is not only about building confidence and trust - a process of a rational standardisation should help avoiding closing a market of cloud computing services because of a dominance of a certain company and/or certain technology. The Commission definitely learnt a lesson from Microsoft and Google cases. The European Telecommunications Standard Institute (ETSI) was obliged by the Commission to work out proposals for adequate standards by 2013. Developing a voluntary certification schemes was considered by the Commission as another necessary step. Standardisation should also regard environmental issues such as energy consumption and carbon emissions[24].

In the Key Action 3 the Commission determined on setting up European Cloud Partnership that - bringing together industry and public administration - should be 'an umbrella for comparable initiatives at Member States level'[25]. ECP's activity will focus on working out requirements for public procurement for cloud computing and advancing joint procurement of cloud computing services by public bodies. The Steering Board of the ECP met for the first time in November 2012 and since that it worked out 'a policy vision document' entitled 'Establishing a Trusted Cloud in Europe'[26], released in 2014. The document predicts two types of actions (Identifying and Creating Best Practices and Consensus Building) oriented for an alignment of policies and legislation for the sake of Single Market.

Within Key Action 2 the Commission planned a development of a model terms for cloud computing service level agreements for a contract between cloud providers and professional

[23] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7.2.2013 (available at http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security, visited 6.3.2015).
[24] CC Strategy, para. 3.2.
[25] CC Strategy, para. 3.5.
[26] Available at http://ec.europa.eu/digital-agenda/sites/digital-agenda/files/discussions/TrustedCloudEurope_3.pdf (visited 6.3.2015).

cloud users. For consumers and small companies intended to propose model contract terms and conditions for issues falling within a proposal on Common European Sales Law. It should be noted that the Commission did not actually propose or even predict any initiatives on hard regulations for cloud computing[27]. A burden of actions lies on soft tools. Legal problems arising from cloud computing in the Commission's view can be solved by regulations of more general character, especially new regulation on data protection.

What is highlighted as specially desired for regulating cloud computing is a better balance between a cloud client and a cloud provider. A hope for improving a regulatory environment of cloud computing is mainly (currently under preparation) General Data Protection Regulation[28]. Draft Regulation predicts that processors will be more accountable towards controllers by assisting them in ensuring compliance in particular with security and related obligations. Failing to fulfil this duty will result in qualifying a processor as a data controller what finally brings an amended scope of a provider's liability (joint controllership)[29]. Article 29 Working Party recommends in this context also guaranteeing a more proactive role for consumers and small businesses in their relations with cloud providers[30].

Another problem, also pointed by Article 29 Working Party, is a disclosure of personal data to authorities (judicial or administrative) from the third countries (outside the EU). In the Working Party's opinion, it should be absolutely prohibited if there is no proper legal ground for such a disclosure: 'proper' in this context means international agreement.

There is also a need for a special care about storing data and information sensitive from a point of view of a country's interests (e.g. data related to public health sector). One idea to deal with data of the highest state important is to create a supranational European Governmental Cloud and establish especially restrictive rules for its functioning. But creating special rules for special cloud does not seem very good idea if analyzed from a standpoint of rationality and cohesion of a law system. Assuming that special rules on data protection in cloud computing, provisions designed solely for European Governmental Cloud would constitute provisions of the second degree of specialization what could probably cause some conflicts not easy to solve on a traditional basis of *lex specialis derogat legi generali*. On the other hand, if there are no some special regulations for cloud computing as such but there are specific regulations for the

[27] CC Strategy, para. 3.3.
[28] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM/2012/011 final - 2012/0011 (COD) (hereafter, Draft Regulation).
[29] See Art. 26, 29 and 30 Draft Regulation.
[30] Art. 29 Working Party Opinion, p. 23.

European Governmental Cloud, they could easily become a point of reference for cloud computing in 'normal' business relations. In my view a solution would be rather creating, if any, a universal regulation that would protect data and interests of all parties engaged in cloud computing regardless their status.

5. Soft framework instead of binding legislation

Cloud computing is very 'democratic' - it can be used either by companies, regardless their size, or by individuals (consumers). Therefore, a scope of a potential legal protection is very broad because it touches various problems in different categories of legal relationships. All the problematic issues of cloud computing are centred in a problem of liability, mainly for protecting privacy, confidentiality, and also legality of data. These problems have been, more or less successfully, resolved by the EU regulations in a more universal sense and they can be applied in case of some legal problems resulting from a cloud computing.

Is there any need for cloud computing law? A specific character of cloud computing makes traditional legal institutions a bit useless, regarding their role for an adequate regulation of contractual relationships. However, many sectors of economy, e.g. financial services, points a need for adopting sector-specific regulations for cloud computing (such as provisions on processing on data protected as banking secrets), accompanying 'general' regulations. But a position rejecting a necessity for special regulations on cloud computing is also worth noticing and justifying.

Even if currently a (moderate) flexibility should be an important characteristic feature for legislations in many areas, it is absolutely a key value for regulating issues related to new information technologies. Rigid regulations that do not follow technological changes quickly enough can bring more damages than benefits for potential users and they can arise a tremendous mess in legal practice what is probably even worse than a total lack of regulations for certain areas. Regarding a method and a procedure of law-making in the EU as well as a number of entities, interested in regulating a cloud computing, but representing totally different interests and points of view, I dare to say that the EU is not able to create a legislation that would be able to develop and insert every single step of an evolution of cloud computing in its technological and business dimension. What is even more, I am rather sceptical if any national lawmaker is able to work out a cloud computing law that would be flexible enough to respond challenges of a development of cloud computing.

Shouldn't public authorities undertake any steps in order to regulate or govern cloud computing? Surely, it cannot be a solution because a lack of regulations does not mean a lack

of real problems. So what instead of 'positive law', 'hard regulations' issued in a normal law-making procedure? A proposal may be a creation of 'soft framework' for cloud computing based on soft law and non-legal measures (mainly technical standards)[31] for resolving legal problems generated by this method of storing digital data. Soft framework should include guidelines, best practices, model terms of contract, voluntary certification schemes and other self-regulatory measures; its necessary ingredients are also compliance programmes. All measures are surely non-binding.

In such a soft framework public bodies loses quits their legislative role but they take on a role of an initiator and a stimulator of activities oriented for establishing a variety of rules of behaviour for cloud computing.

Soft framework as a concept of organising relationships of clients and providers of cloud computing features with flexibility, dynamism and openness as basic values and advantages. But it also has some crucial disadvantages. The very first is a lack of legal safety. On one hand binding regulations are quite often criticized for their strictness and toughness but on the other - a common wish, expressed by societies, seems to be an expectation to regulate (legislate) as many parts of real (and virtual) life as possible. Legislation is claimed to be a synonym for legal safety, although actually this safety is hardly ever total. In order to defend a soft framework for cloud computing it must be pointed that various soft measures create at least 'safe harbours' and a consent upon a certain issue within a particular group of entities sharing the same interests, which is a core of self-regulation, may be a very strong guarantee for successful enforcement of norms of conduct.

The second disadvantage of soft framework for cloud computing may be (but not necessarily is) a multitude of norms of conducts, their categories, types, localization as well as an outstanding number and different nature of norm-making bodies. Assuming that the EU with its CC Strategy implements actually, this feature can be easily noticed within EU 'policy' on cloud computing - it is a real jungle of papers, notices, strategies, initiatives, implementing measures, etc. subject to never ending process of consultations. The whole concept and its enforcement does not seem to be transparent.

As suggested above the EU seems to follow a pattern of soft framework (as defined earlier), the Commission does not show any pressure on adopting a 'hard' legislation on cloud computing. This approach, although imperfect, is the most rational. New technologies, including ones related to cloud computing, will always be a step ahead of lawmakers and there

[31] N. Gleeson, I. Walden, *It's a jungle out there?: Cloud computing, standards and the law*, "European Journal of Law and Technology" 2014/2.

is nothing we can do about it. In my view a soft framework as a concept for governing relationships connected to services of cloud computing just allows for an honorary defeat of a lawmaker.

Summing up, a soft framework as a concept bears some resemblance to cloud computing (as a concept). Therefore, it is absolutely justified to say that regulations on cloud computing in the EU are still high in the sky. And they probably will never go down to the earth.

Chapter 3

CONNECTED TV AS THE TECHNOLOGICAL PUZZLE CALL FOR A REFORM OF AUDIOVISUAL MEDIA SERVICES DIRECTIVE[1]

Katarzyna Klafkowska-Waśniowska

Ph.D, Assistant professor at the European Law Department, Faculty of Law and Administration, Adam Mickiewicz University in Poznań

Keywords: *Smart TV, connected TV, European audiovisual policy, audiovisual media services, on-demand services.*

Abstract: *The Audiovisual Media Services Directive replaced the basic EU law act applicable to broadcasting the Television Without Frontiers Directive. The AVMSD was to be the technology neutral act, but the advent of smart TV has underpinned the existing regulation. In the article the basic functions of smart TV and the current discussion concerning the potential reform of the AVMSD is discussed. The starting point is the possibility of accessing different services offering audiovisual material, via connected devices. The article highlights the issue of the scope of the "audiovisual media service" focusing on the non-linear audiovisual media service to exemplify which services fall outside of the AVMSD. Furthermore, the example of the protection of minors is chosen to demonstrate what are the legal consequences if the service is not an audiovisual media service. As the smart TV is the puzzle for the legislator the main elements of this puzzle are referred to in this article.*

1. The Audiovisual Media Services Directive and connected TV - facts, functions, future?

The Audiovisual Media Services Directive (AVMSD) was enacted in 2007, and codified in 2010[2]. The AVMSD is the successor of the Television Without Frontiers Directive (TWF),

[1] This article is part of the research project financed by the NCN (Narodowe Centrum Nauki in Poland) No 2012/07/B/HS5/03921.

[2] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) *OJ L 95, 15.4.2010, p. 1–24.*

the solutions of which were found to be a success in the internal market for broadcasting services[3]. The backbone[4] of the AVMSD is the country of origin principle and the minimum possibilities for derogation from this principle, together with the provisions setting minimum standards for protection of public order, minors, protection of viewers as consumers and the promotion of EU works. The country of origin principle in the AVMSD served as a model for the E-commerce Directive[5] which aimed at the harmonisation of certain aspects of provision of the information society in general, leaving the issues related to the content of those services aside. The constant development of broadcasting services and new types of audiovisual services required analysis of to what extent the changes in the current EU legal framework are needed. In its Communication on the Future of European Regulatory Audiovisual Policy, the Commission reminded five basic principles for the regulatory action: it should be the minimum necessary to achieve a clearly defined political goal, guaranteeing legal certainty and technological neutrality, and enforced as closely as possible to the concerned operator[6]. As noted in the Communication, the take-up of broadband services at the time was slower than expected, yet the preparations for the revision of the TWF Directive began. As a result, the AVMSD introduced the concept of "audiovisual media service" covering the traditional television (linear) services and the emerging on-demand (non-linear) services. The general objective of the AVMSD was the emergence of common programme production and distribution market, and ensuring fair competition without the prejudice to the public interest.[7] The application of the basic tier of rules originating in the TWF Directive to on-demand service providers was a novelty in the majority of the Member States. It was a significant change in the regulation of audiovisual services, that is why it has been observed with great interest. The first report of the application of the AVMSD[8], drew the attention to the new stage of convergence and the development of "connected devices".

[3] Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions, *The Future of European Regulatory Audiovisual Policy* COM (2003) 784 final, p.6.
[4] European Parliament Resolution of 22 May 2013 on the Implementation of the Audiovisual Media Services Directive (2012/2132(INI)) at A.
[5] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, Official Journal L 178, 17/07/2000 p. 1-16.
[6] *The Future of European Regulatory Audiovisual Policy* p.6.
[7] Recital 2 of the Preamble to the AVMSD.
[8] *Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the application of Directive 2010/13/EU "Audiovisual Media Services Directive". Audiovisual Media Services and Connected Devices: Past and Future Perspective.* COM (2012) 203 final.

The commonly used terms: connected TV, smart TV, and hybrid TV describe the possibilities offered by those devices that are able to receive broadcasts, and at the same time access the Internet. Traditionally, broadcasting was a service consisting of offering audiovisual programmes by means of specific technology (terrestrial, satellite or cable communication) to an end user, using a TV receiver. The possibility of offering the broadcasts on the Internet, mainly the retransmission of offline transmissions, may be perceived as an intermediary stage of the convergence in the area of audiovisual content. At the same time new types of services such as video-on-demand, near-video-on demand or pay-per-view, or platforms for sharing audiovisual content developed. Connected TV combines these services and ads new possibilities. On the one hand it provides new possibilities for developing the television offer, on the other, new possibilities for viewer not to use linear services to access audiovisual content[9]. The main feature of connected TV is the integration of broadcasting and broadband internet[10]. Not only television receivers, but also PC's or smartphones are connected devices. Alongside television channels, the viewer has access to catch-up TV offer of the broadcasters, audiovisual content offered by on-demand service providers or over-the-top services[11], social media portals, electronic press or different websites, for example of producers of goods and services advertised alongside the audiovisual content. The actual possibilities depend on the device and integrated software, in some cases only access to the limited number of services is allowed and in other the access to is not restricted[12]. The use of connected TV is linked to the access to broadband internet. The Commission predicts that the use of connected devices will become more and more popular. The number established in 2012 was 40,4 million of such devices. It is predicted that they will become a majority in EU households in 2016[13]. In Poland it was assessed, that 1 million users had a TV offering Internet connection, the important point is however how many of them actually used that function[14]. In EU the highest usage was reported in UK, but it is still low -11%[15].

---

[9] A.Scheuer *Convergent Devices, Platforms, and Services for Audiovisual Media. Challenges set by Connected TV for the EU Legislative Framework*, "IRIS Plus" 2013/3, p.9.

[10] *Audiovisual Media Services and Connected Devices: Past and Future Perspective.* p. 9; European Broadcasting Union. *Principles for Connected and Hybrid Television in Europe.*15.04.2011. p. 1.

[11] European Parliament Resolution of 4 July 2013 on connected TV (2012/2300(INI)), at K.

[12] Green Paper *Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values.* COM(2013) 231 final, p. 9.

[13] Green Paper *Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values...* p. 3.

[14]It has been pointed that consumers often do not use of the functions that a device offers.
K.Zalewski, S.Celmer, J.Firlej, E.Murawska-Najmiec, A.Woźniak, *Telewizja hybrydowa: szanse, zagrożenia I wyzwania regulacyjne*. KRRiT, Warsaw, May 2013, http://www.krrit.gov.pl/Data/Files/_public/Portals/0/publikacje/analizy/tv-hybrydowa_raport_2013-05-16_2_def-2.pdf, p. 4. Accessed 02.10.2015.

[15] Green Paper *Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values...* p. 3.

In its evaluation of the application of the AVMSD, the Commission pointed to the main challenges among which achieving a level playing field, control over advertising and audiovisual content and the impact of connected TV on the effectiveness of measures promoting the European works and the protection of minors are mentioned. The main puzzle seems to be how to "maintain a consistent level of protection across different media environments while taking into account their respective specificities". The Commission emphasized that the boundaries between broadcasting and over the top delivery of content become blurred[16]. In the European Parliament's opinion, the consumers will distinguish less and less between linear and non-linear services. In its Resolution on the implementation of the audiovisual media services directive, the Parliament has called the Commission to address particularly the uncertainties surrounding the use of the term "on-demand audiovisual media services" and to establish a clearer definition of this term[17]. The concern here is both the consistency in EU Legislation, application in the Member States and the development of hybrid services. Assessing the AVMSD in the context of connected television the Parliament found that its provision do not yet reflect the ongoing technological convergence. The graduated regulation of linear and non-linear services will become less important but the regulatory objectives of the AVMSD such as promoting diversity of opinion and the media, protecting human dignity and protecting children, encouraging the providers to ensure accessibility for visually and hearing impaired and safeguarding fair competition retain their importance to the society[18]. The possibility of the reform of the AVMSD has been voiced expressly by the Parliament[19] and submitted for a debate by the Commission in its Green Paper on the convergence in the audiovisual world[20]. The discussion continues in the framework of the new Digital Market Strategy[21].

This article highlights the issue of the scope of the "audiovisual media service" focusing on the non-linear audiovisual media service to exemplify which services fall outside of the AVMSD. Furthermore, the example of the protection of minors is chosen to demonstrate what are the legal consequences if the service is not an audiovisual media service.

---

[16] *Audiovisual Media Services and Connected Devices: Past and Future Perspective.* p.10

[17] *European* Parliament resolution on the implementation of the Audiovisual Media Services Directive at 31-49, European Parliament Resolution of on Connected TV at 69.

[18] Ibidem at.M-O.

[19] European Parliament resolution of 12 March 2014 on Preparing for a Fully Converged Audiovisual World (2013/2180 (INI)), at 36.

[20] Green Paper *Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values...*

[21] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions, *A Digital Single Market Strategy for Europe*, COM(2015) 192 final p. 10-11.

2. What does "all audiovisual media services" mean?

The possibility of accessing a number of services with one device is not new, if we consider for example the use of PCs. The concern with smart TV is that this "one" device should be the television receiver, taking into account that television is a regulated field in the EU. The expectations of viewers as to the regulatory protection are mentioned in the AVMSD, as one of the premises for expanding its scope[22]. It is assumed that in order to, among others, avoid distortion of competition and improve legal certainty, at least the basic tier of coordinated rules should apply to all audiovisual services. Yet the balance of interests of viewers' protection, freedom of speech, safeguarding other fundamental rights and the emerging state of the market for new audiovisual services resulted in the exclusion of a number of services. Therefore, the assumption that the basic set of rules should apply to "all audiovisual media services" is true only with respect to the services covered by the AVMSD. "Audiovisual media service" means a service within the meaning of the Treaties, which is provided under editorial responsibility of a media service provider and the principal purpose of which is the provision of programmes, in order to inform, entertain or educate to the general public by electronic communications networks[23]. A non-linear audiovisual media service is characterised as the offering of programmes on the basis of a catalogue, for viewing at the moment individually chosen by user, and at his request (on demand). Many questions were posed as to the scope of the AVMSD from the very beginning[24], and in Poland the doubts led to protests against the planned implementation of AVMSD, because of the potential "censorship" of Internet.[25] The limits of the AVMSD's scope can be illustrated with three examples important from the perspective of development of connected TV: the electronic versions of newspapers, the various internet portals with video content, for example not suitable for minors, and the video sharing platforms.

---

[22] Recital 24 of the AVMSD.

[23] Art. 1 (1) a) i) of the AVMSD.

[24] See for example: A.Breitschaft, *Evaluating the linear/non-linear divide - are there any better factors for the future regulation of audiovisual media content?* Ent.L.Rev, 8/2009 p. 293; H.Lutz. *The distinction between linear and non-linear services in the new proposal of the audiovisual media directive C.T.L.R. 12/2006, p. 143, S.Ridgeway, The Audiovisual Media Services Directive - what does it mean, is it necessary and what are the challenges to its implementation? C.T.L.R 4/2008 p. 109.*

[25] Media reports on the discussion on the implementation of the AVMSD: *Ministerstwo: nie koncesjonujemy Internetu.* Rzeczpospolita z *15.03.2011, http://www.rp.pl/artykul/627186.html; Ministerstwo Kultury o nowelizacji ustawy medialnej: nie wprowadzamy koncesjonowania Internetu, Gazeta Prawna http://prawo.gazetaprawna.pl/artykuly/495987,ministerstwo_kultury_o_nowelizacji_ustawy_medialnej_nie_wprowadzamy_koncesjonowania_internetu.html; Nowela ustawy o TV – internauci boją się wprowadzenia cenzury, źródło PAP, Gazeta Prawna z 16.03.2011 http://www.gazetaprawna.pl/wiadomosci/artykuly/496303,nowela_ustawy_o_rtv_internauci_boja_sie_wprowadzenia_cenzury.html* ; accessed 02.10.2015.

The electronic versions of the newspapers are expressly excluded in the preamble of the AVMSD[26]. Taking into account the problems experienced in different Member States[27], and the referral of the Austrian *Vervaltungsgerichtshof* to CJEU, seeking clarification of the basic definitions provided for in the AVMSD[28], the application of AVMSD in this area is far from clear. Taking advantage of the possibilities of internet communications the electronic versions of newspapers also offer audiovisual content. It is equally true for the electronic versions of newspapers published also in print, and for solely internet news portals. The aim of the AVMSD is to cover only those services, that have as their principal purpose the provision of programmes (videos). The distinction between text and moving images indeed seems to characterise well the differences between the traditional television and newspapers, but is questionable in the internet communication.

The question of comparability of programmes communicated as part of on-demand services to broadcast programmes, which formed part of the referral of the Austrian court, is vital also when it comes to classification of other services than internet news portals. A very interesting case was examined by the Office for Communication (Ofcom) in the UK, and concerned a portal Urban Chick Supremacy Cell. While considering the appeal from the decision of ATVOD[29], that found the portal to be a regulated ODPS (on demand programme service). Ofcom disagreed, pointing that the service consisted of videos picturing sado-masochistic activities lacking a complete narrative, frequently being short sections of a longer activity offered to niche audience and therefore incomparable to broadcast programmes. Furthermore Ofcom found the difference in viewing experience with comparison to broadcasting, pointing to the 'blogging-template' and web-like navigation manner, and concluded that it would be unlikely for the viewers to consider themselves watching a programme service competing with television programmes[30]. The case demonstrates the difficulty with determining which of the internet video portals should be classified as the audiovisual on demand services. Inconsistencies in the application of concept of audiovisual

[26] Recital 28 to the AVMSD.
[27] J. Metzdorf *The Implementation of Audiovisual Media Services Directive by National Regulatory Authorities. National Responses to Regulatory Challenges.* JIPITEC 2/2014.
[28] Request for a preliminary ruling from the Verwaltungsgerichtshof (Austria) lodged on 18 July 2014 — New Media Online GmbH v Bundeskommunikationssenat, Case C-347/14, concerns art. 1 (1) a) i) and 1 (1) b of the AVMSD, Opinion of Advocate General Szpunar of 01.07.2015.
[29] Authority for Television on-Demand.
[30] Ofcom's Decision in the Appeal by Itziar Bilbao Urrutia for the service The Urban Chick Supremacy Cell in respect of ATVOD's Notice of Determination dated 6 January 2014 p.20-23; http://stakeholders.ofcom.org.uk/enforcement/video-on-demand-services/

media services are very likely, also due to the fact that for example in Polish implementation of AVMSD there is no "comparability" criterion in the definition of a "programme"[31].

As stems from the Ofcom decision, and recital 24 of the AVMSD, the concept of audiovisual on demand service is linked to the competition between new media services and broadcasting. It can be read from the preamble of AVMSD, that the services consisting of the provision or distribution of audiovisual content generated by private users are not in competition with the broadcasters, and as such should not come within the scope of the Directive. It should be agreed, that more importantly in case of video sharing platforms there is a problem of satisfying a condition of editorial responsibility, defined as the effective control over the selection of the programmes and their organisation in a schedule or a catalogue[32]. The question who has the control over content, mirrors the problems of qualification of hosting providers who can invoke the liability exemption according to E-commerce Directive[33], and is growing with the expansion of the cloud based TV services. The European Parliament called for the application of the concept of media services in such a way that the need for regulation by the Member States is determined, *inter alia* on the basis of editorial responsibility[34]. In the subsequent resolution on the convergence in the audiovisual world, the Parliament has described the "content gateway" as any entity which acts as an intermediary between audiovisual content providers and end-users, and brings together, selects and organises a range of content providers and provides an interface for users to access the content[35]. The Parliament emphasised the issues for consideration in the field of competition law, but the focus on "content gateway" seems equally important from the perspective of searching for the providers who should be responsible for meeting the standards required by the AVMSD.

[31] Art 4(2) of the Radio and Television Act 1992: *programme" shall mean a set of moving images with or without sound (audiovisual programme) or a set of sounds (radio programme) constituting, in terms of its content, form, designation or authorship, an individual item within a programme service or a catalogue of programmes made available to the public by a media service provider as part of the on-demand audiovisual media service, hereinafter the "catalogue". http://www.krrit.gov.pl/en/for-broadcasters-and-operators/legal-regulations/*

[32] A. Giurgiu, J.Metzdorf, *Smart TV – Smarte Regulierung?* In: *Big Data & Co., Neue Herausforderungen für das Informationsrecht*. J., Taeger (ed.), Oldenburg, Germany 2014, p. 713.

[33] In depth analysis of this problem in K.Klafkowska-Waśniowska *Nowe formy audiowizualnych usług medialnych a przesłanka "odpowiedzialności redakcyjnej" w dyrektywie o audiowizualnych usługach medialnych.* „ZNUJ" 2014/2, p. 112-133.

[34] European Parliament Resolution on connected TV at 3.

[35] European Parliament Resolution on Preparing for a Fully Converged Audiovisual World at J and 2.

3. Public policy objectives in the European audiovisual policy and obligations of media service providers

When discussing the priorities of European regulatory policy in the audiovisual sector, the Commission pointed to paramount objectives of general interest such as: cultural and linguistic diversity, the protection of minors and human dignity and consumer protection[36] and suggested that the rules developed within this framework may be seen as policy objectives valid for any kind of audiovisual services[37]. This logic is implemented in the AVMSD provisions, but the level of regulation is different for linear and non-linear services. The rules on the general ban of incitement to hatred, identification obligations, audiovisual commercial communication, the provisions on the accessibility for persons with visual or hearing impairment and the provision on the "media chronology" constitute the so called basic tier, applicable to all audiovisual media services.

The rules concerning two objectives highlighted in the recent EU documents[38], the promotion of European works, and the protection of minors are formulated differently for linear and nonlinear services[39]. These objectives seem to be fundamentally different. The protection of minors in the context of the free movement may justify the derogation from the country of origin principle, while the promotion of European works does not[40]. It is not included neither in art. 3 (2) a), nor in art. 3 (4)a)i) of the AVMSD. Setting the standard for the protection of minors has a broad context of creating a "safe" electronic environment, but also to eliminate the possible barriers in the free flow of audiovisual content. In the promotion of European works, the emphasis is on the stimulation of the European audiovisual industry, production and distribution of content, *vis a vis* the audiovisual content imported from third countries, notably the U.S. It is worth noting that the European Parliament has recommended the deregulation of the areas of AVMSD in which the legislative aims are not being achieved[41]. Although the Parliament expressly referred only to the removal of the quantitative rules on advertising in linear services, its recommendation may be contrasted with the critique of the AVMSD provisions on the promotion of European works, and the results presented in the Commission's

[36] *The Future of European Regulatory Audiovisual Policy.* p. 3.
[37] *Ibidem* p. 13.
[38] European Parliament Resolution on the Implementation of the Audiovisual Media Services Directive at 31-49, European Parliament resolution on connected TV at H and 44, European Parliament Resolution on Preparing for a Fully Converged Audiovisual World at 37 and 40.
[39] Art. 12 and 13 of the AVMSD.
[40] The Judgment of the Court of 29th May 1997 in case C-14/96, Paul Denuit, on the basis of the Television without Frontiers Directive.
[41] European Parliament resolution on Preparing for a Fully Converged Audiovisual World… at. 49.

report[42]. The Parliament is however of the opinion, that the support for high levels of sustained investments in original European content remains a key priority[43].

4. Protection of minors

The issue of protection of minors from harmful content has been barely mentioned in the Commission's first report on the application of the AVMSD. The focus of the Commission was on the issue of protection of minors with respect to audiovisual commercial communication and new initiatives in the field[44]. The European Parliament has however linked the issue of protection of minors to the problems of convergence and use of connected devices[45]. If the services are not audiovisual media services, but for example ordinary internet portals, electronic versions of newspapers, blogs or the content distributed by social media users, the rules that can be found in EU law are restricted to the Directive 2011/92/EU on combating the sexual exploitation of children and child pornography[46], art. 4 a) i), 16 (1) e) of the E-Commerce Directive, and the recommendations of non-binding character[47]. As far as the audiovisual content that may be legally communicated to the public is distributed in those "other services", the solutions for protecting minors were suggested first in the Council Recommendation of 1998[48], and then in the European Parliament and Council Recommendation of 2006[49]. The emphasis in the E-Commerce Directive is on the self-regulation, particularly on the development of codes of conduct and this approach follows the guidelines set in the Recommendation on the protection of minors and human dignity of 1998. It has been pointed in the 2006 Recommendation, that though self-regulation of audiovisual sector has proved to be an effective additional measure, it is not sufficient to protect minors from messages with

[42] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. First Report on the Application of Articles 13, 16 and 17 of Directive 2010/13/EU for the period 2009-2010 Promotion of European works in EU scheduled and on-demand audiovisual media services COM/2012/0522 final.
[43] European Parliament resolution on Preparing for a Fully Converged Audiovisual World… at.H.
[44] *Audiovisual Media Services and Connected Devices: Past and Future Perspective*. P.5, 7-9.
[45] European Parliament resolution on Preparing for a Fully Converged Audiovisual World… at F and G.
[46] Directive 2011/92/EU of 13.12.2011 on the on combating the sexual exploitation of children and child pornography replacing Council Framework Decision of 22.12.2003. 2004/68/JHA, O.J. L 335/1.
[47] Together with the Safer Internet Programme Decision 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies.
[48] Council Recommendation 98/560/EC of 24 September 1998 on the development of the competitiveness of the European audiovisual and information services industry by promoting national framework aimed at achieving a comparable and effective level of protection of minors and human dignity. OJ L 270, 07.10.1998, p. 48-55.
[49] Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry OJ L 378, 27.12.2006, p. 72–77.

harmful content[50]. The conclusions in the Recommendation 2006 are that the Member States should take up among others, actions aimed at raising awareness and media literacy among viewers, especially minors, facilitating the identification of quality content for minors and reporting the illegal content on the Internet. The service providers on the other hand should for instance consider development of filtering systems and content labelling of materials distributed over the Internet and co-operate with regulatory, self-regulatory and co-regulatory bodies of the Member States with the aim of exchanging best practices and harmonization of existing solutions.

The harmonization of protection of minors in electronic communication services pictures as follows. The E-commerce Directive is applicable to all information society services, including those services that, as above demonstrated, fall out of the scope of the AVMSD. With respect to the protection of minors, art. 3 (4)a)i) AVMSD is identical to art. 4 a) i) of the E-Commerce Directive, and allows for derogation from the country of origin principle. There are however no provisions in the E-commerce Directive that would create obligations for service providers distributing content harmful to minors. According to art 16(1) e) of E-Commerce Directive, the Commission and Member States should encourage the drawing up of codes of conduct regarding the protection of minors and human dignity. According to the AVMSD, the content that might seriously impair the physical, mental, or moral development of minors cannot be broadcast (art.27 (1)), and as far as the programmes which are likely to impair the physical, mental or moral developments of minors is concerned, the broadcasters are obliged to ensure that minors will not normally hear or see such broadcasts (art. 27 (2)). There is no ban on dissemination of programmes that might seriously impair the physical, mental or moral development of minors in art. 12 applicable to nonlinear services, but such content can only be made available in such a way as to ensure that minors will not normally hear or see such on-demand audiovisual services. Restrictions on the dissemination of content harmful for minors in EU law apply thus only in case of services covered by the AVMSD. It is worth noting, that the AVMSD does not specify in the exhaustive way what kind of content might seriously impair the developments of minors, but establishes the obligation of access control. The examples of pornography and gratuitous violence are specified in art. 27 (1). In some Member States concerns are raised as to the different standards accepted for example in the UK and the Netherlands[51]. On the other hand some commentators find originally in the TWF Directive, the

[50] Recommendation 2006, at 12.
[51] *For Adults Only. Underage access to online porn. A research report by the Authority for Television On Demand.* 28.03.2014, http://www.atvod.co.uk/uploads/files/For_Adults_Only_FINAL.pdf p. 22.

source for developing of a uniform EU-wide concept of pornography[52]. In the area of protection of minors, the role of EU law is primarily to prevent the distortions on the internal market, as the protection of minors lies within the sphere of public policy shaped by the Member States[53]

The evaluation of the state of play has been initiated by the Commission's 2011 Report Protecting Children in the Digital World[54].With respect to co/self-regulation systems in the context of AVMSD, the Commission noted the variety of actions in the Member States, and concluded that this reflects the difficulties with the development of consensual policy approach. The Commission's conclusion is not the undisputed need for the action at EU level, but the weaker statement that it might *"build on the best practices of the Member States and reach economies of scale for the ICT sector"* and at the same time, help the children[55]. The Commission's Report does not yet address the problems of smart TV, rather the communication on the Internet in general. It is clear that the set of rules for broadcasting differs substantially from the rules that have been developed for the services outside the AVMSD's scope. The European Broadcasting Organisation proposed, also in 2011, the set of principles for connected and hybrid television in Europe. With respect to protection of minors, EBU stresses that hybrid systems must not be used to circumvent broadcast regulation. According to rule 12 national regulation and self-regulation on the protection of minors must be respected and hybrid systems should facilitate the parental control[56]. For that purpose, according to the European Parliament , the Electronic Programme Guide functions might be used[57]. In case of EPGs the question of the AVMSD's scope returns. EPGs are covered by the definition of the audiovisual media service, as long as they accompany programmes, within the meaning of AVMSD[58]. It seems however, that focusing on EPGs is aimed at solving problems also of services falling outside the AVMSD. One of the difficulties lies in the fact that EPG services may be provided not only by media service providers, but for example by the connected devices manufacturers[59]. The big

[52] J. Ukrow, in: O.,Castendyk, E. Dommering, A. Scheuer, *European Media Law.* Alphen a/d Rijn 2008, p. 711.
[53] Judgment of the CJEU of 14.02.2008 in case C-244/06 Dynamic Medien Vertriebs GmBH p. Avides Media.
[54] Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the application of the Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity and of the Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and online information services industry, COM (2011)556 final.
[55] *Ibidem* p.11.
[56] European Broadcasting Union. *Principles for Connected and Hybrid Television in Europe.* 15.04.2011.
[57] *Resolution on Connected Television* at 44.
[58] Recital 23 of the Preamble to AVMSD.
[59] A.Scheuer *Convergent Devices, Platforms, and Services for Audiovisual Media. Challenges set by Connected TV for the EU Legislative Framework*…p. 19.

questions: which services, which providers, what obligations and how to enforce them, remain still open for the discussion.

5. Conclusions

The 1st Report on the application of the AVMSD brought suggestion of a change. The technological neutrality principle as applied in the AVMSD is apparently not enough at the next step of convergence, exemplified by the growing popularity of connected TV. The European Parliament is active in the field of suggesting what work should be done: evaluating the linearity criterion and the areas where the AVMSD turned out to be a success and where not. It is a difficult task. The TWF Directive was found to be a success, and the reports on the AVMSD are so far inconclusive in parts concerning non-linear services. The Feedback Paper[60] published by the Commission to summarize the answers submitted in the consultation process on the convergence in the audiovisual world, offers some insights into the Member States, regulatory authorities, industry and consumer representatives point of view. Those views on the issues raised in the article such as the scope of the AVMSD or the particular issue of the protection of minors are diverse. On the latter, as the Commission's document summarizes, the opinion that the current provisions are sufficient and appropriate is not frequently argued by Member States, but it is by some stakeholders[61]. If the solution put in the simplest words is not to allow minors to access seriously harmful content, then the idea seems applicable to all types of services and content, but there is still a long way to achieve this goal. As far as the determination of the scope of the AVMSD and the possible extension to other service providers, or even device manufacturers is discussed, the recurring theme is whether there is the competition between the providers subject to the AVMSD or not. This approach is adopted in the AVMSD, as it encompasses the on-demand services that may partially replace television broadcasting[62]. I would argue however, that the focus on the services that might replace broadcasts and compete for the same audience is inadequate when dealing with connected TV issues. The old TV receivers might be replaced by new ones, but this is only the symbol of changes in the audiovisual sector.

[60] Summaries of replies to the public consultation launched by the Green Paper "Preparing for a Fully Converged Audiovisual World: Growth, Creation and Values". https://ec.europa.eu/digital-agenda/en/news/publication-summaries-green-paper-replies
[61] *Ibidem*, p. 84
[62] Recital 69 of the AVMSD.

Chapter 4

INTERMEDIARIES CAUGHT BETWEEN A ROCK AND A HARD PLACE - THE CASE OF WEBSITE BLOCKING AND NO GENERAL OBLIGATION TO EXERCISE CONTROL OVER THE USER-GENERATED CONTENT

Daria Katarzyna Gęsicka

Ph.D, Assistant Professor, Nicolaus Copernicus University in Toruń, Department of Civil and International Trade Law, ul. Władysława Bojarskiego 3, 87-100 Toruń, Poland, dgesicka@umk.pl

Keywords: *permanent injunctions, intermediaries, proportionality, users' rights*

Abstract: *Intermediaries are in the middle of every single act of online communication. The term "intermediary' does not refer to homogenous group of service providers. In fact, it is used to describe entities who provide services necessary for an act of electronic communication to be successful including telecommunication service providers, online connectivity providers and entities providing their services by electronic means. Although, the e-commerce directive refers only to specific categories of intermediaries, such as providers of the following services: mere conduit, caching or hosting, the more our lives depend on technology, the more significant the role of every single intermediary becomes. The seriousness is particularly visible in relation to injunctive orders following a decision on the merits of the case (also referred to as 'permanent injunctions') such as website blocking orders the aim of which is to prevent future online infringements. As protective measures, the injunctions are subject to the proportionality evaluation and cannot lead to the effect that would be contrary to the provisions of the article 15 of the E-commerce Directive.*

The paper discusses the phenomenon of website blocking orders against intermediaries, including orders against the so-called 'innocent providers', and the boundaries of the orders. This particular type of an injunction serves as a trigger point for the analysis of the injunctions paradigm and engagement in a debate concerning rights of the users. The injunctions are

currently holding a prominent position in the EU legal system as a consequence of the decision of the Court of Justice of the European Union in Telekabel v. UPC case and the judgment handed down by the European Court of Human Rights in Delfi v. Estonia case. Thus the author of this paper concentrates on the analysis of the abovementioned decisions and their implications for the sphere of users' rights (such as freedom of expression) and the freedom of business activity.

1. European regulation on permanent injunctions

1.1. Introductory remarks

The recent five or six years have witnessed fascinating growth of claims for website blocking injunctions in private litigations, mostly civil litigations in copyright or trademark or personal rights disputes. In numerous cases the claims have been addressed against access providers (or Internet connectivity providers) who, in general, from the tort law perspective cannot be held liable for third party content disseminated on the Internet. Therefore, the category of intermediaries is sometimes referred to as "innocent providers". At the same time, the providers being in the core of electronic communication, have the might to stop, or at least, attenuate the tsunami of the infringements; however, the might is subject to technological restrictions.

The tools which enable claimants to petition for an injunction are implementations of article 8 (3) of the InfoSoc Directive and the third sentence of article 11 of the Enforcement Directive[63] into the national legal systems. The first of the provisions is a vehicle that can be applied in copyright and related rights infringement cases, whereas the latter – in cases of the infringement of intellectual property rights, except for the copyright or related rights infringement due to the *lex specialis derogate legi generali* rule. Both provisions oblige each and every Member State to ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe intellectual property rights, nevertheless according to recital 23 of the Enforcement Directive the conditions and procedures relating to such injunctions should be left to the national law of the Members States. Whereby the provision the Member States are equipped with a huge margin of freedom as far as procedural and material premises of the protective measures are concerned. As explained in

[63] Directive 2004/48/EC of the European Parliament and of the Council of 29.4.2004 on the Enforcement of Intellectual Property Rights, Official Journal of the European Union L 195 of 2.6.2004, p. 16-25, referred to as the Enforcement Directive.

recital 31 of the Infosoc Directive[64] services provided by intermediaries may be applied in a wrongful manner leading to infringing activities and due to the fact that intermediaries are in the middle of all electronic activity, they might find themselves in the best position to bring such activities to an end. The challenging task to introduce provisions that would allow the right holders to receive an order against 'an intermediary who carries a third party's infringement of copyrighted work or other protected subject matter in a network', regardless of whether an intermediary can be held liable or not in accordance with article 5 of the Infosoc Directive, was entrusted with the Member States. The wording of the recital suggests that injunctions should be treated as independent measure that can be applied irrespective of intermediaries' liability. Therefore it seems justified to label the measure as 'in rem injunctions'[65]; however the statement requires further justification which is presented in due course in the paper.

1.2. Permanent injunctions against intermediaries

The most significant element of the above-cited provisions is an indication of an addressee of the injunction. According to the provisions, the injunctions should be addressed to 'intermediaries whose services are used by a third party'. Also, what may be, and actually, has been, a subject of controversy is the manner in which the injunction should be formulated. To be more specific, it has been dubious whether the order has to indicate the exact measures that need to be introduced by an intermediary in execution of the judgment or it is acceptable to leave the choice of measures to an intermediary with the reservation that the chosen measure should be proportional, efficient and deterring in accordance with the wording of article 11 of the Enforcement Directive. Although the Enforcement Directive seems to hold the key to the former question – about the addressee of the injunction – it does not say a word on the latter.

The term 'intermediaries whose services are used by a third party' was partially explained by the Court of Justice of the European Union (CJEU) in the justification of the judgment of 12.7.2011 in *L'Oreal versus eBay case*[66]. One of the preliminary questions addressed to the Court was whether article 11 of the Enforcement Directive allowed national courts to issue an

[64] Directive 2001/29/EC of the European Parliament and of the Council of 22.5.2001 on the harmonization of certain aspects of copyright and related rights in the information society, Official Journal of European Union L 167 of 22.6.2001, p. 0010-0019, referred to as the InfoSoc Directive.

[65] The term was coined by Martin Husovec who claims that the construction of the injunctions is based on the theoretical framework for an old Roman concept of 'in rem actions', also known as 'actio in rem negatoria'. M.Husovec, *Injunctions against Innocent Third Parties: The Case of Website Blocking*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2013/4, p. 116.

[66] Court of Justice (Grand Chamber): C-324/09, *L'Oréal SA, Lancôme parfums et beauté & Cie SNC, Laboratoire Garnier & Cie, L'Oréal (UK) Ltd v. eBay International AG, eBay Europe SARL, eBay (UK) Ltd, Stephen Potts, Tracy Ratchford, Marie Ormsby, James Clarke, Joanna Clarke, Glen Fox, Rukhsana Bi,* 12.7.2011, JO C 471, 12.7.2011, par. 130.

injunction against an operator of a website, such as an operator of an online marketplace, by means of which the rights to copyrighted content or related rights had been infringed. Therefore, the referring courts asked for an interpretation of the term 'intermediaries whose services are used by a third party'. In paragraph 128 of the judgment CJEU replied that 'an injunction' referred to in the third sentence of article 11 can be addressed to an operator of an online marketplace because injunctions stipulated in the provision differ from injunctions referred to in the first sentence of the same article. The exact words of the CJEU were as follows:

'*For the purpose of determining whether the injunctions referred to in the third sentence of Article 11 of Directive 2004/48 also have as their object the prevention of further infringements, it should first be stated that the use of the word 'injunction' in the third sentence of Article 11 differs considerably from the use, in the first sentence thereof, of the words 'injunction aimed at prohibiting the continuation of the infringement', the latter describing injunctions which may be obtained against infringers of an intellectual property right*.'

Having said that, CJEU implied that the scope of entities against whom injunctions can be issued is broader than the scope of entities who can be held liable for an infringement. To justify its opinion CJEU presented the following contextual argumentation:

'*a restrictive interpretation of the third sentence of Article 11 of Directive 2004/48 cannot be reconciled with recital 24 in the preamble to the directive, which states that, depending on the particular case, and if justified by the circumstances, measures aimed at preventing further infringements of intellectual property rights must be provided for*.'

In addition to that, in paragraphs 130 and 131 CJEU referred to the wording of article 18 of the E-commerce Directive[67] by saying the following:

'*That interpretation is borne out by Article 18 of Directive 2000/31, which requires the Member States to ensure that court actions available under their national law concerning information society services' activities allow for the rapid adoption of measures designed to terminate any alleged infringement and to prevent any further impairment of the interests involved. An interpretation of the third sentence of Article 11 of Directive 2004/48 whereby the obligation that it imposes on the Member States would entail no more than granting intellectual-property right holders the right to obtain, against providers of online services, injunctions aimed at bringing to an end infringements of their rights, would narrow the scope*

[67] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), Official Journal of the European Union L 178 of 17.7.2000, p. 0001-0016, referred to as the E-commerce Directive.

of the obligation set out in Article 18 of Directive 2000/31, which would be contrary to the rule laid down in Article 2(3) of Directive 2004/48, according to which Directive 2004/48 is not to affect Directive 2000/31.'

However, as rightfully stated by M. Husovec[68], the framework of intermediaries' liability is an undefined concept, which makes it difficult to determine to whom and which of the two injunctions can be addressed. In fact, in most Member States it is required that an intermediary could be held liable for indirect infringement in order to grant an injunction against the intermediary. Internet connectivity providers, such as the defendant in the *Telekabel v. UPC* case, cannot be held liable neither for direct infringement nor for the indirect one due to lack of causative chain of events. Direct linkage between the injunctions and tortious liability seems to be one of the thresholds for the grant of a website-blocking injunction. For example, section 97A of the British Copyright, Designs and Patents Act of 1988 and the High Court case law provide that there are four threshold conditions for the grant of an injunction:

- first, an intermediary is a service provider within the meaning of reg. 2 of the E-commerce Directive;

- second, users and/or the operator of the website in question infringe the claimant's copyrights;

- third, users and/or the operator of the website use the defendant's services to infringe the claimant's copyrights; and

- fourth, the defendant has actual knowledge of the infringement[69].

The conditions were reviewed by the High Court in *Cartier Interntional AG v. British Sky Broadcasting Ltd.*[70] where the court referred to art. 11 of the Enforcement Directive and held that under section 37 (1) of the Copyright, Designs and Patents Act of 1988 there were four threshold conditions for the grant of an injunction, and presented a very similar set of rules to the one cited above. The conditions are as follows:

---

[68] M. Husovec, *Injunctions against Innocent ...,* p. 117.

[69] R. Arnold, *Website-blocking injunctions: the question of legislative basis*, „European Intellectual Property Review" 2015/10, p. 625.

[70] High Court of Justice: *Cartier International AG v British Sky Broadcasting Limited, British Telecommunications plc, EE Limited, Talktalk Telecom Limited, Virgin Media Limited* [2014] EWHC 3354 (Ch), 17.10.2014. Access: http://international.westlaw.com/result/default.wl?tofrom=%2fsearch%2fresult.aspx&mt=UKIP09&origin=Search&sri=17%2c18&utid=12&db=UKIP-CASELOC%2cIP-RPTS-ALL&rlt=CLID_QRYRLT585440415510&method=TNC&service=Search&eq=Welcome%2fUKIP09&rp=%2fWelcome%2fUKIP09%2fdefault.wl&sp=intjagie1-000&query=%22CARTIER+INTERNATIONAL+AG+V+BRITISH+SKY+BROADCASTING+LTD%22&vr=2.0&action=Search&rltdb=CLID_DB8762040415510&srch=TRUE&sv=Split&fmqv=s&fn=_top&rs=UKIS1.0 Date of access: 4.10.2015

- first, the defendant is an intermediary;

- second, users and/or the operator of the website in question infringe the claimant's intellectual property rights;

- third, users and/or operator of the website use the defendant's services to do that;

- fourth, the defendant has actual knowledge of this.

Also, in the justification of the judgement, the court explained that although the fourth condition was not contained in art. 11 of the Enforcement Directive, it followed from art. 15 of the E-commerce Directive[71]. At the same time German[72] or Austrian laws do not recognize such requirement and allow for the injunctions to be addressed against internet connectivity providers. The same questions concerning the addressee of the injunctions and their content were considered by the CJEU.

1.3. Intermediaries in legal systems of the EU Member States

Being the domain of national law, secondary liability doctrines differ significantly from each other[73]. The differences between national laws of the different Member States can be exemplified by dissimilar legal classifications of websites based on user-generated content such as MySpace or DailyMotion, or YouTube. For an instance, on 22.6.2007 French Tribunal de Grand Instance (TGI) in Paris decided that the operator of MySpace website does not provide hosting services to its users, hence it is a content provider as decisions concerning structure of the website and the presentation manner of users' content were made by the operator. Also, TGI determined that the operator had gained benefits coming from advertisers whose advertisements had been disseminated on the website, which might have influenced the decision. Whereas, Belgian Court of Commerce in its decision of 31.8.2008 in *Lancôme versus eBay* case classified the operator of eBay online marketplace as a hosting services provider[74]. On one hand, in the Member States which have opted for limited scope of secondary liability the injunctions are considered to be a filler in the underdeveloped doctrines of tortious liability. On the other, in those Member States which have adopted a broad concept of secondary

[71] High Court of Justice: *Twentieth Century Fox Film Corp, Universal City Studios Productions LLLP, Warner Bros Entertainment Inc, Paramount Pictures Corporation, Disney Enterprises, Inc., Columbia Pictures Industries Inc. v British Telecommunications Plc* [2011] EWHC 1981 (Ch), 28.7.2011. Access: http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/28_07_11_bt_newzbin_ruling.pdf date of access: 4.10.2015

[72] R. Arnold, *Website-blocking injunctions* ..., p. 629.

[73] The difference has been described comprehensively in a study *Injunctions in Intellectual Property Rights* by European Observatory on Counterfeiting and Piracy. Access: http://ec.europa.eu/internal_market/iprenforcement/docs/injunctions_en.pdf Date of access: 20.2.2015.

[74] D. K. Gęsicka, *Wyłączenie odpowiedzialności dostawców usług sieciowych za treści użytkowników*, Warszawa 2014, p. 250-251.

liability, the injunctions are perceived as, sometimes disproportional, extension of the liability[75]. For example, in Poland in accordance with article 422 of Polish Civil Code a permanent injunction can be issued only against parties such as a better (a person who induces the direct infringer), an ancillary (a person who provides the direct infringer with tools, knowledge and other means required to commit an infringement) and a person who benefited from the infringement. Hence, the addressee of the injunction can be only a 'guilty' intermediary, including the entities within the meaning of the articles 12-15 of the Polish Act of 18.7.2002 on Provision of Services by Electronic Means[76]. Similarly, in Czech Republic it is necessary for an intermediary to participate in court proceedings as a party in a dispute so that the court could address an injunction to the intermediary[77]. At the same time, in Italy it is admissible for a court to order a permanent injunction against any intermediary whose services are used by a third party to infringe irrespective of an intermediary's liability for the infringement[78].

1.4. The definition of the term 'intermediary' in *Telekabel v. UPC* case[79]

The differences concerning the scope and premises of the liability of an intermediary are deeply rooted in national legal systems of the Members States, therefore, so far, the CJEU has not succeeded in harmonization of the Members States secondary liability doctrines which does not mean that the CJEU has capitulated in the harmonization field.

In its quite recent decision in *Telekabel v. UPC* case CJEU once again challenged the question of the interpretation of the term 'intermediaries whose services are used by a third party', albeit the preliminary question concerned Internet connectivity providers who are placed entirely outside the scope of the direct or secondary liability. The decision has sparked off

[75] M. Husovec, *Injunctions against Innocent ...,* p. 117.
[76] Act of 18.7.2002 on Provision of Services by Electronic Means, Journal of Laws 2013, item 1422 (pol. ustawa z dnia 18.7.2002 o świadczeniu usług drogą elektroniczną, Dz. U. 2013, poz. 1422). The provisions are the implementation of the articles 12-15 of the E-commerce Directive.
[77] The Study *Injunctions in Intellectual Property Rights* by European Observatory on Counterfeiting and Piracy, p. 97-98.
[78] See the decision of the Court of Milan, 16.1.2009. The court granted an injunction against a national distributor of a publication where the distribution lead to trademark infringement, although the distributor was found to be entirely innocent due to the fact that according to Italian law press or periodicals distributors are obliged to accept any publication without any evaluation of its content. Cited after the Study *Injunctions in Intellectual Property Rights* by European Observatory on Counterfeiting and Piracy, p. 13, 105-106.
[79] Court of Justice: C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgeschellschaft GmbH,* 27.3.2014, JO C 192, 27.3.2014.

various reactions, by some[80] it has been perceived as a harbinger of censorship, by others[81] as a well-balanced reaction to the challenges brought about by new technologies.

The reasoning of CJEU was based on three arguments: the autonomous nature of the injunction, the exclusive character of copyrights as well as the functional and systemic interpretation of the article 8 (3) of the InfoSoc Directive. Having taken all the above aspects into consideration, CJEU held (in paragraphs 37 and 39 of the judgment) that:

'*Directive 2001/29 requires that the measures which the Member States must take in order to conform to that directive are aimed not only at bringing to an end infringements of copyright and of related rights, but also at preventing them. Such a preventive effect presupposes that the holders of a copyright or of a related right may act without having to prove that the customers of an internet service provider actually access the protected subject-matter made available to the public without their agreement*'.

Consequently, the conclusion was that the provision in question must be interpreted as meaning that a person who makes protected subject-matter available to the public on a website, without the consent of the right holder, should be deemed, for the purpose of Article 3 (2) of the InfoSoc Directive, the one using services provided by the intermediary to users who access that subject-matter, and therefore the intermediary should be considered an intermediary within the meaning of Article 8 (3) of the InfoSoc Directive. The decision in *Telekabel versus UPC* case seems to stay in line with the previous CJEU's decision in *LSG-Geschellschaft versus Tele2* case[82] where the court came to the following conclusion:

'*access providers which merely provide users with Internet access, without offering other services such as email, FTP or file-sharing services or exercising any control, whether de iure or de facto, over the services which users make use of, must be regarded as 'intermediaries' within the meaning of Article 8(3) of Directive 2001/29*'.

Thus, having adopted a contextual reading of the provision, CJEU has once again concluded that injunctions referred to in the article 8 (3) are not related to liability of an intermediary. The European Commission and Advocate General Kokott in *Frisdranken* case

[80] D. Nagel, *Network Blocking in the EU: A Slippery Slope to (Third Party) Censorship? How the CJEU Missed to Give a Crucial Guidance in his Judgement on UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, C-314/12, Decision 27 March 2014*, „Computer Law Review International" 2014/4, p. 113-116.
[81] I. Wróbel, *Odpowiedzialność dostawcy dostępu do Internetu jako pośrednika, którego usługi są wykorzystywane w celu naruszenia praw autorskich lub pokrewnych – glosa do wyroku Trybunału Sprawiedliwości z 27.03.2014 r. w sprawie C-314/12, UPC Telekabel Wien GmbH przeciwko Constantine Film Verleih GmbH i Wega Filmproduktionsgesellschaft GmbH*, „Europejski Przegląd Sądowy" 2015/4, p. 31-40.
[82] Court of Justice (Eight Chamber): C-557/07, *LSG-Geschellschaft zur Wahrnehmung von Leistungschutzrechten GmbH versus Tele2 Telecommunication GmbH*, 19.2.2009, JO C 107, 19.2.2009.

(C-119/10) adopted identical reading of the provision[83]. Even though the two stands were taken in relation to the twin provision of the article 8 (3) of the InfoSoc Directive – the third sentence of the article 11 of the Enforcement Directive – they support CJEU's argumentation presented in the *Telekabel versus UPC* case. As a consequence, by saying that injunctions are a separate protective measure which is unrelated to neither direct nor indirect liability CJEU managed to escape the dead end of lack of harmonization in the field and, at the same time, generated an ardent discussion on its relation to the conclusions reached by CJEU in *Scarlet Extended* case[84].

In opinion of the author of the paper, CJEU's interpretation of the term 'intermediary' should meet with approval. Acceptance of the alternative – the strict interpretation of the term – would in turn have adverse effect on the efficiency of right holders' protection, thus would result in contradiction of the *erga omnes* character of intellectual property rights. Also, the interpretation stays in line with wording of the Enforcement Directive and only such an interpretation can guarantee sufficient level of copyright protection in face of challenges of new technologies. Direct infringers, entities who make works available to the public in an illicit manner, quite often escape consequences of application of a blocking order addressed to their hosting services provider by removing their content to another server or changing the domain, which makes the orders ineffective. However, the approval of the interpretation of the term intermediary is not followed by unconditional approval of any injunction. Purposes set out in the Digital Agenda such as economic growth of e-services and development of an information society require that the content of an injunction be proportional.

1.5. The content of a permanent injunction

Another element of a permanent injunction which has constituted a subject of heated discussion is the content of an injunction, in particular, the extent to which courts are entitled to designate the scope of technical measures to be undertaken by an intermediary in order to prevent future infringements. In trial to formulate the order courts need to take the following factors into consideration: technical character of a particular measure, its proportionality[85] and fundamental rights of three groups of interests: right holders, intermediaries and users.

---

[83] M. Husovec, *Injunctions against Innocent ...,* p. 117.

[84] Court of Justice (Third Chamber): C-70/10, *Scarlet Extended SA v. Sociéte belge des auteurs, compositeurs et éditeurs SCRL* (SABAM), 24.11.2011, JO C 771, 24.11.2011; referred to as *Scarlet Extended* case. The two cases, however, differ significantly as far as their subjects are concerned. The *Telekabel versus UPC* case refers to "innocent providers", whereas in the Scarlet Extended case CJEU dealt with hosting services providers.

[85] For more profound analysis of proportionality of website blocking see P. Sevola*, Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2014/5, p. 116-138.

As far as technical character of a particular measure is concerned, the measures which have already been developed and applied in analogous case-law are far from perfection. The technical measures which are ordered most frequently are as follows:

- DNS blocking which consists in preventing the domain name server from translation of certain domain names. Application of the measure results in blocking of access to certain websites;

- IP address blocking which consists in blocking certain IP addresses applied by the server where the illicit content is stored;

- Deep Packet Inspection (DPI) which allows for blocking of entire websites or URLs[86].

Each and every method can be quite easily circumvented, e.g. by the use of encryption, thus none of them is entirely efficient[87], yet from the point of view of internet connectivity providers their application can result in unjustified limitation of the freedom of business activity, in particular if the injunctions become an extensively used protective measure.

In general, execution of an injunction might constitute a burden which, if not proportionate, may function as a barrier for undertaking business activity. For this reason, it is of utmost importance for an injunction to be proportional. According to P. Sevola[88] in the Member States' legislation and jurisprudence there are four approaches, categorized by region and orientation, towards website blocking that can be distinguished. These are as follows[89]:

a. Expanding approach, adopted by UK courts[90] – the content of injunctions is not only to block IP addresses or DNS of a direct infringer, but its scope is extended to those IP addresses or DNS the main role of which is to enable or facilitate access to the infringing content[91];

b. Mixed approach in Nordic Countries – courts in Nordic Countries have a tendency to balance fundamental rights and all interests carefully, therefore most injunctions concern particular illegal content or those websites which are directly infringing; nevertheless, rights of users of the Internet as a group of interest are rarely a subject of consideration. In vast

[86] M. Husovec, *Injunctions against Innocent …*, p. 122.
[87] See also paragraph 60 of the CJEU's judgment in *Telekabel v. UPC*.
[88] P. Sevola, *Proportionality of Website* Blocking …., p. 123-124.
[89] See also in D. K. Gęsicka, *Nakazy sądowe kierowane do pośredników w komunikacji elektronicznej*, Kwartalnik Prawa Prywatnego 2015/2, p. 452-454.
[90] For the study of evolution of the injunctions see R. Arnold, *Website-blocking injunctions*, p. 628-629.
[91] High Court of Justice: [2012] EWHC 723 (Ch.), no. HC110C03290, *Golden Eye (International) Limited, Ben Dover Productions, Celtic Broadcasting Ltd, Easy on the Eye, DMS Telecom Limited, Gary Baker, Harmony Films Limited, Justin Ribeiro dos Santos t/a Joybear Pictures, Orchid MG Limited, Kudetta BVBA, RP Films Limited, Sweetmeats Productions t/a S.M.P, SLL Films Limited, Terence Stephens t/a One Eye Jack Productions versus Telefónica UK Limited*, 26.3.2012. Access: http://www.bailii.org/ew/cases/EWHC/Ch/2012/723.html Date of access: 9.3.2015

majority of cases, the courts issued injunctions against those intermediaries who could be held liable for secondary infringement[92];

c. Divergent approach in Benelux region – on the one hand scholars and researchers from the University of Amsterdam in their study on injunctions proved that blocking an entire website constitutes a disproportional measure and the approach was adopted by the Court of Appeal in the Hague[93], on the other courts in Belgium are of the opinion that it is proportional and justified to impose on an intermediary an obligation to block or monitor all domains including a particular word or phrase even if the domain does not exists at the time of the issuance of the order[94].

The differences between the Member States hamper harmonization process. For this reason, there are numerous judgments by means of which CJEU strives to unify rules governing the content of injunctions. Recently, CJEU has had an opportunity to express its opinion on the Austrian legal institution known as *Erfolgsverbot* – an injunction which obliges an intermediary to achieve a particular goal such as preventing future infringements, leaving the choice of the technical measures to an intermediary. In the manner, Austrian courts shift the responsibility to balance all interests at stake onto intermediaries. CJEU decided that the institution is consistent with EU law. Although the institution is typical for Austrian legal system, it can constitute a precedent which might designate the direction for courts in the other Member States to follow in their own judgments. The measure is convenient for the right holders as the burden of proof connected with the choice of the proper measure and its efficiency is transferred onto intermediaries. It can be agreed that intermediaries' filed of expertise as far as blocking measures and their application are concerned is much greater than their knowledge among judges, however most intermediaries, in particular small and medium-size entrepreneurs in most cases are not acquainted with intricacies of copyright law and human rights protection. Therefore, CJEU's opinion should not be welcomed with too much of enthusiasm unless we want to scare the intermediaries off and inhibit the development of that particular sector of serviced. Also, the courts of the Member States need to remember that enforcement of an injunction should not amount up to the general obligation to monitor a third party content.

[92] P. Sevola, *Proportionality of Website Blocking* ..., p. 123-124.
[93] *Gerichtshof's-GravenHage* (Court of Appeal in The Hague): no. 200.105.418–01, *Ziggo B.V. i XS4ALL Internet B.V.*, 28.1.2014, par. 5:17–5:21. Access: http://www.boek9.nl/files/2012/2012-11-13_Hof_Den_Haag_Tele2_en_KPN_v_Brein.PDF Date of access: 20.2.2015.
[94] P. Sevola, *Proportionality of Website Blocking*, p. 125.

2. European regulation on general obligation to monitor the third party content

Article 15 (1) of the E-commerce Directive stipulates that Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity. According to CJEU article 15 precludes the Members States from introducing legal provisions that would impose on intermediaries an obligation to carry out active monitoring of data transmitted by their users[95]. *Ratio legis* of the provision was a reasonable assumption that it was impossible to filter away all illegal content[96]. Also, introduction of such an obligation would lead to legalization of preventive censorship which would be contrary to article 10 of the European Convention on Human Rights and Fundamental Freedoms of 1950[97]. Apart from designation of aims that should be achieved by legislative power in the Member States, the provisions of article 15 of the E-commerce Directive demarcate frames of its application by courts. Therefore, courts cannot issue an order that would result in astricting intermediaries, within the meaning of articles 12-14 of the E-commerce Directive, to monitor all or most of the content uploaded and made available to the public by their users[98]. Acceptance of the contrary stand could yield an infringement of fundamental rights of both: intermediaries – freedom of business activity – and users – freedom of privacy. Infringement of the latter could appear due to the fact that in order to block or disable content of specific users it would be necessary to gather and process personal data of each and every user, such as their IP numbers.

Since article 15 of the E-commerce Directive mentions only three specific categories of intermediaries, which are providers of mere conduit, caching, and hosting services, and one may wonder whether a court can impose such a general obligation to monitor user-generated content on those intermediaries who are beyond the scope of articles 12-15 of the E-commerce Directive. Referring to the *a fortiori* argument, the author of this paper is of the opinion that if entities who may have significant influence on the user-generated content and as such can commit indirect infringements are exempted from obligation to monitor all or most of the data

[95] Court of Justice: *Scarlet Extended* case, par. 36.
[96] Court of Justice: C-314/12, *UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Wega Filmproduktionsgeschellschaft GmbH*, par. 60.
[97] Convention for the Protection of Human Rights and Fundamental Freedoms of 4.11.1950, Rome. Access: http://www.echr.coe.int/Documents/Convention_ENG.pdf Date of access: 9.3.2015.
[98] Court of Justice (Third Chamber): C-70/10, *Scarlet Extended SA v. Sociéte belge des auteurs, compositeurs et éditeurs SCRL* (SABAM), par. 38-40, 50-51.

transmitted by means of their services, all the more the innocent intermediaries should not be asked to do so. Another reasoning may lead to lack of proportionality.

2.1. The ECHR decision in *Delfi AS versus Estonia* case

The main question by which ECHR was challenged in *Delfi AS versus Estonia* case[99] concerned the place of fundamental rights in the hierarchy of European legal norms. The Court had to decide whether the interference of Estonian courts with Delfi's freedom of expression was justified in the light of article 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms. Therefore, the ECHR had to determine whether the interference – having held Delfi liable for comments coming from anonymous users even though the publisher had expeditiously removed the illegal content in accordance with the notice-and-take down procedure – was prescribed by law and necessary in a demographic society, in particular whether it was indispensable to protect third party's reputation. In order to assess the first premise of legitimate limitations to the freedom of expression it was essential that the law be formulated with a sufficient precision for a citizen, so that he/she could foresee legal consequences of his or her conduct. According to ECHR Estonian regulation on publisher's liability for publication of defamatory comments was precise and clear enough to pass the legality test. Having answered that part of the question, ECHR had also to determine whether protective measures taken against the intermediary had been necessary in a democratic society taking into consideration the following four factors: the content, measures applied by the applicant to prevent or remove infringements, access to liability of direct infringements – authors and consequences of domestic proceedings for the applicant.

ECHR concluded that although the notice-and-take down procedure was an efficient and necessary measure, in the face of anonymity of users it was required to improve prior filtering procedure. Thus, the media company should have either restricted ability to publish comments only to registered users or applied more efficient *ex-ante* filtering measures. Moreover, ECHR elucidated yet another questionable issue – subsidiarity of liability of an intermediary in terms of proportionality of protective measures. Having invoked its judgment in *Krone Verlag versus Austria* case[100], ECHR agreed that the liability shift did not constitute a disproportionate

[99] European Court of Human Rights: application no. 64569/09, *Delfi AS v. Estonia*, 10.10.2013. Access: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{"itemid":["001-126635"]} Date of access: 8.3.2015

[100] European Court of Human Rights: application no. 39069/97, *Krone Verlag GmbH & Co. KG v. Austria*, 11.12.2003. Access: http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-61538#{"itemid":["001-61538"]} Date of access: 8.3.2015.

interference with the media's company freedom of expression due to the fact that at times if it was not for the liability shift, the applicant would never have his/her claims satisfied as, in general, intermediaries are more solvent than a mere user. Nevertheless, the statement does not seem to be indubitable since natural persons undertaking blog-writing activity or running a small, simple chatroom are not necessarily more solvent than authors of infringing comments[101].

3. Conclusions

Copyright or related rights holders, intermediaries and users represent three different groups of interests. Complexity of the tripartite relation makes it impossible to satisfy all needs of the parties at the same level. In order not to get lost in the Bermuda Triangle, courts need to contemplate consequences of issuance of a permanent injunction with peculiar caution so that the subtle balance is not disturbed. Therefore, the assessment of proportionality criteria is obligatory. In the quest for appropriate balancing of the interests, courts should pay more attention to function of an injunctive. An injunction can be treated either as a preventive measure restricted to individual effect, thus a measure applied to eliminate particular infringements once and for all, or a preventive measure in a broader meaning, the main value of which is to educate all users on consequences of an infringement and to show them that their infringements will not go unnoticed. Bearing in mind the fact that fulfillment of the first goal is unrealistic, which has been acknowledged by CJEU in the judgment in *Telekabel v. UPC case*, the key point is to satisfy the latter goal and at the same time guarantee high standard of protection to right holders, which might as well be achieved by proper education. Yet another important issue is the existence of stable and consistent jurisprudence concerning intermediaries. Provided that intermediaries know what to expect from courts and which legal aspects they should pay attention to, the development of their services should not be slowed down as they would be able to work out standard procedures of dealing with blocking orders. However, the research carried out by M. Favalle, M. Kretschmer and P. C. Torremans[102] shows that in the current state of affairs one cannot speak of a consistent EU copyright jurisprudence. Instead, the Court compensates for its lack of expertise in copyright law (or other specific branch of law) by enabling so called "judicial learning", which is by assigning the copyright

[101] See also N. Zingales, *Virtues and Perils of Anonymity. Should Intermediaries Bear the Burden?*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2014/5, p. 155- 171.
[102] M. Favalle, M. Kretschmer and P. C. Torremans, *Is there a EU Copyright Jurisprudence. An empirical analysis of the workings of the European Court of Justice*, available at Social Science Research Network. Access: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2643699 Date of access: 4.10.2015.

cases to certain Judges Rapporteurs and Advocates General. Bearing in mind the conclusions reached in the study one cannot help but wonder if such method of compensating for the lack of pre-existing expertise is applied in terms of a clash between copyright protection or human rights on one hand and new technologies on the other. Although electronic communication bears significant resemblance to the traditional ones, the technological intricacies can affect greatly decisions issued by the courts. Therefore, judges and AGs who are appointed to cases in which such a clash appears need to be fluent in both clashing disciplines.

Chapter 5

PROTECTION OF MINORS AND HUMAN DIGNITY IN THE INFORMATION SOCIETY: EU AND US PERSPECTIVES

Magdalena Konopacka

Associate Professor, University of Gdańsk, Department of European and Comparative Law, Bażyńskiego 6, 80-952 Gdańsk, Poland, m.konopacka@ug.edu.pl.

Keywords: *Information society, Human dignity, Protection of minors*

Abstract*: Negative aspects of the information society were first noticed in early 90's, with the dawning of the Internet era. The article gives an overview of European initiatives undertaken and European courts' judgments delivered over the last two decades, contrasting them with eminent U.S. Supreme Court decisions. According to the author, predominance of soft law, case law and self-regulation does not in itself impede protection, given that all stakeholders act with the intention to effectively monitor and eradicate threats.*

1. The New Media

The XXI century is the era of digital technology[1], which has already become indispensable for the vast majority of developed societies and will to enhance our work and everyday life, at the same time sneaking into the spheres of our privacy. The undeniable profits are thus necessarily deterred by the possibly insurmountable loss. Human dignity and privacy – the values which throughout centuries have been cherished in democratic societies – are put at hazard. The most delicate and most important members of every society – children – are

[1] With all the positive (primarily educational) and negative consequences (violence, pornography, invasion of privacy) of this phenomenon for the minor. The „global e-village" is by no means a safe haven for a human being, especially one so fragile - and thus worthy of special protection - as a child. Professor Brodecki depicted the position of an individual as central and involving interactions with other members of the society, the law and the Internet. See: Z. Brodecki, *Epilog. Technologie i prawo w społeczeństwie wiedzy* [in:] *Świątynia w cyberkulturze. Technologie cyfrowe i prawo w społeczeństwie wiedzy*, A. M. Nawrot, Z. Brodecki, p. 94. There is a threat, however, that a human being, entire societies and the law will stand powerless, faced with the unstoppable flow of non-filtered, unimportant, false or harmful information filling the Internet every second. When almost everyone wants (and can) be the editor not less than the addressee of content (raging from Wikipedia entries, blogs and forums to on-line video games), service providers and website administrators do not manage or are not permitted by the law to shut the floodgates to instances of hate-speech or violence.

endangered by illicit content, especially in the jungle-like environment of the Internet.[2] At the same time, any attempt to limit this negative influence of information available on TV or on-line, might be counter-argued by the defenders of free speech. The latter is undeniably one of the foundations of democracy, therefore governments must make sure that their activities aimed at protection of minors and human dignity do not hinder the right of citizens to impart and receive information. All the above considerations must be taken into account, and in every case fair balance must be struck between competing rights of individuals.

2. Hazards inherent in the Information Society

The ideals to which Europe adheres have their roots in the philosophy of ancient Greece, Roman law and Christian religion, gradually adjusted to modern times by the philosophy of Humanism and Enlightenment, especially the French Revolution[3]. They are currently being faced with the typically post-modernistic abundance of information and multitude of communication channels.

The European Union has followed the examples of Japan and the United States in creating a regulatory framework for what is called "information society"[4]. The Commission White Paper of as early as 5 December 1993 attached special attention to the role of new technologies in the social life[5]. In view of the almost universal access to almost uncontrolled content, the Commission found it necessary to safeguard not only the competitiveness and freedom of provision of services within the EU, but also the fundamental freedoms in the audiovisual domain, with co-operation between the public and the private sector[6]. The phenomenon of convergence of different media, seriously accelerating the attainment of the Single Market, requires a new regulatory approach[7].

---

[2] Not less of a threat are 3G mobile phones, which – along with the Internet and traditional media – may not only distribute illicit content, but are also perfect devices addicting the youth to a global brand. The phenomenon of „convergence" is used to create an army of perfectly uninformed consumers.

[3] See also: A. Scharf: *The Media and the European Model of Society* [in:] *European Audiovisual Conference*, Birmingham, 6-8 April 1998, Papers and Documents.

[4] The plan *on national information infrastructure was created in the US already in September 1993*. It resulted in the creation of global network, which – with some exceptions – led to the evolution of an extraordinary phenomenon: a truly single, though not uniform, internet society.

[5] COM(93)700 final

[6] See: Report of Commissioner Bangemann *„Europe and the planetary Information Society"* of 26 May 1994; Commission Communication *„Europe's Way to the Information Society",* COM(96) 347 final of 19 July 1994 and Resolution of the European Parliament of 19 September 1996, O.J. 1996, C 320, p. 164; See also: W. Sauter: *EU Regulations for the Convergence of Media, Telecommunications, and Information Technology: Arguments from Constitutional Approach?* [in:] Zentrum für Europäische Rechtspolitik an der Universität Bremen Diskussionpapier 1/98, pp. 3-5. Specific regulations on convergence are provided for In the Commission Green Paper of 3 December *1997 on convergence* COM(97) 623.

[7] See: M. Bangemann: *A new World Order for Global Telecommunications – The Need for an International Charter*, speech of 8 September 1997 delivered during Telecom Inter@ctive97 in Geneva,

The Commission has on many occasions stressed the changing context of the problem of protection of minors and human dignity[8]. Television is more and more focused on editing rather than broadcasting. This is possible thanks to digital technologies, which make possible offering diverse services, e.g. near video-on-demand or pay-per-view. At the same time, the problem of insufficient number of available frequencies is solved, which results in an almost unrestricted choice of services and programmes. A second, even more advanced, group of digital services are on-line services, which enable a user to not only receive, but also submit information, available on demand to virtually everyone in the world.

In view of the above, protection of minors and dignity proves to be a serious challenge to all sectors offering such services, creating a need for restricted governmental intervention. The citizens of the European Union being members of the knowledge-based society - are at the gates of vast resources and knowledge, which generally should not be restricted[9]; this global information infrastructure may, however, turn them into victims rather than beneficiaries. This is why certain level of public control must be accepted.

António Vitorino, former Internal Affairs and Justice Commissioner, formulated those dangers in a speech during a conference "Internet and the Changing Face of Hate"[10]. Materials inciting to hatred, racism and xenophobia, promoting violence and discrimination, or containing all kinds of pornography can easily be found in the Cyberspace. European experience of the World War II makes the European Union and the Council of Europe particularly concerned about any signs of such activity; and the widely discussed and revealed problem of child abuse is also an issue of fundamental human rights and respect.

There have been many cases of neo-Nazist and racist activities reported. Hatred is often directed towards ethnic minorities, recently of Arabic origin, in particular as a reaction to Al-Qaida attacks. One example of judicial intervention is the case of YAHOO!, which – upon lawsuit filed by organisations fighting anti-Semitism - has been forced to ban Nazi materials as contrary to French public law. This did not, however, apply to a server located in the United States, where, based on the First Amendment – such content was still allowed and being presented.

---

http://www.ispo.cec/be/infosoc/promo/speech/geneva.html; see also: W. Sauter: *EU Regulations for the Convergence of Media…, supra,* pp. 6-8.

[8] Commission working document – consultations on the Green Paper on protection of minors and human dignity in audiovisual and information services, SEC(97) 1203, Brussels, 13.06.1997.

[9] See: *„Democracy and the information society in Europe"*, publication of the DG Education and Culture.

[10] A. Vitorino, *Statement at the occasion of the Conference*: *„The Internet and the Changing Face of Hate"*, p. 1, Berlin, 26.06.2000, http://www.europa.eu.int/rapid/start/cgi

Another, recent example, with possible repercussions for the Internet and other media, is that of 3 organisations within Vlaams Blok, which by decision of Hof van Cassatie of 9 November 2004 (confirming the judgment of the Court of Appeal of Gent of 21 April 2004) were convicted on the grounds of the antiracism law of 30 July 1981 for giving assistance to a political party that has manifestly and repeatedly incited to discrimination and xenophobia, esp. towards citizens of Moroccan and Turkish origin. The Court referred to different kinds of publications of the Vlaams Blok, each of them propagating hatred and xenophobia. This started a debate over the accessibility of Vlaams Blok to public media. The Flemish Broadcasting Act states that the programmes of the VRT (the Flemish public broadcasting organisation) should contribute to a democratic and tolerant society (Art. 8 § 3) and the Executive Agreement between the VRT and the Flemish Government of 7 November 2001 obliges it to "contribute to mutual understanding, increase tolerance and stimulate community relations in a pluri-ethnic and multicultural society". This might mean that the right of the political party to freely express its views, as well as conduct election campaign in the mass-media cannot be enforced[11].

At the same time, every individual's activity can be easily traced in this virtual world, which makes possible the creation of a precise profile, reflecting that person's political convictions, religious practices and beliefs, consumer habits. Thus, another important issue arises – that of data protection and governmental interest in collecting this data. Of course, this may sound disturbingly similar to the famous George Orwell's *1984;* but - as fictitious as this threat may seem – it should not be disregarded[12].

Negative opinion as regards governmental control of activities in the Cyberspace has been expressed by John Perry Barlow, who in his rather romantic vision of the Internet proclaims it a „new world", ruled by the principle of unrestricted freedom of speech, and to which no regulatory framework can effectively be applied[13]. A much more realistic point of view is that of Graham Smith, who calls suggestions such as Barlow's wishful thinking rather than actual knowledge on the subject. Smith doesn't see a threat in public, regulatory control over the Internet; he contends, however, that execution of such laws might be problematic, subject to all jurisdictions of the world.[14]

---

[11] Source: Iris 2005/1 – DV.

[12] Certain safeguards have been proposed by the Human Rights Watch in a Report "*Silencing the Net*: *The Threat to Freedom of Expression On-line"*, Vol. 8, No.2, May 1996.

[13] B. Dority, *Ratings and the V-chip, The Humanist*, May/June 1997, pp. 16-19.

[14] G. Smith, *Internet law and regulation,* London 1996. Jurisdiction can in many cases be difficult to determine. One of the few attempts to overcome these difficulties is the British Computer Misuse Act 1990, which stipulates that this Act shall be the law applicable to acts committed by a person located within the UK territory or using a computer located in this territory at that time; it is however sufficient that the act itself takes place within this

3. Children's Rights and Human Dignity

Human dignity has not been defined and is not safeguarded by a single act of international or supranational law, being a notion discussed in legal theory as well as constitutional law and human rights. In philosophy; this notion has been discussed throughout centuries; from Hipereides in Ancient Greece (who perceived a human being as divine reflection), to Kant (who assumed an individual's internal morality and thus dignity), to give just two examples. It is nonetheless undisputable that the "inherent dignity of an individual human being" is a root-notion, from which the ideals of freedom, equality and justice (fairness) are derived.

Neither the European Convention for the protection of Human Rights and Fundamental Freedoms (ECHR), nor the International Pact on Civil and Political Rights contain any provisions referring expressly to the notion of human dignity; whereas such reference is made in Article 1 of the Universal Declaration of Human Rights. Also the Charter of Fundamental Rights provides that the European Union „is founded on the indivisible, universal values of human dignity, freedom, equality and solidarity (…)". The entire Chapter I is entitled „Dignity", and its Article 1 stipulates that: Human dignity is inviolable. It must be respected and protected". In the context of the information society, human dignity is defined by way of giving an exemplary list of threats it is exposed to in the sphere of audiovisual and information services.

As regards EU competence in counteracting criminal activity, also in the Internet, Article 67 (3) TFEU – which opens Title V Area of Freedom, Security and Justice - stipulates that "the Union shall endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws". According to Article 167 TFUE, EU action is merely „aimed at encouraging cooperation between Member States and, if necessary, supporting and supplementing their action" – among others - in the audiovisual sector.

Protection of children, whose dignity is unquestionable and perhaps even elevated due to their vulnerability, is the objective of many international documents, such as: the Geneva Declaration of 1924, the UN Declarations of 1948 and 1959, the International Pact of 1966 (Articles 23 and 24), to name but a few. Undeniably, the most universal is the UN Convention of Children's Rights done at New York in 1989, which proclaims the child's right to the

territory. See on this subject: E. Diamond, S. Bates, *Law and order comes to cyberspace*, MIT Technology Review 98, October 1995, pp. 22-33.

peaceful development of personality in the spirit of ideals expressed in the United Nations Charter, in particular in the spirit of peace, dignity, tolerance, freedom, equality and solidarity.[15]

Also, the EU Charter of Fundamental Rights[16] in Article 24(1) stipulates that children are entitled to such protection and care as is necessary for their good. They can also freely express their opinions, which should be taken into account in matters regarding them, considering their age and maturity. Equally important is the fact, that, according to section 2 of this Article, public authorities and private institutions undertaking any activity with respect to children must give priority to the best interests of a child. In the context of the information society this means for example the necessity to create a catalogue of content otherwise legal, but that should be prohibited as harmful to physical, moral and psychological development of minors.

If we look at the cradle of the information society and the new media with highly developed marketing techniques – American research studies present a full range of harmful cognitive, social and health effects of illicit content on unbiased and trustful children, not neglecting possible educational value of the media.[17] Particularly alarming is the well-established opinion of American healthcare organisations based on over four decades of research according to which viewing entertainment violence (in the media in general, not to mention on and off-line video games) can lead to increases in aggressive attitudes, values and behaviour, particularly in children, and that there is a very close causal link between the two.

4. Freedom of Expression

In the context of freedom of expression, Jürgen Habermas concisely pointed out the role of the media in this respect: the media should enable social discourse, also between authorities and citizens, initiate social education, enforcing the individual's right to receive and express opinions (within the limits not harming another individual's freedoms, for example human dignity, privacy, or minors) and resist external forces attempting at restriction of those freedoms[18]. John Stuart Mill in his essay *„On freedom of thought and speech"* even argued

[15] More on international protection of children, specifically in private law relationships, see: M. Konopacka, *Res privata* [in:] *Komparatystyka kultur prawnych*, Z. Brodecki, M. Konopacka, A. Brodecka-Chamera, Wolters Kluwer, Warszawa 2010, p. 188 et seq.
[16] The Charter has become binding upon entry into force of the Treaty of Lisbon on 1 December 2009.
[17] A. Gentile & C. A. Anderson, *Violent Video Games: Effects on Youth and Public Policy Implications* [in:] Handbook of Children, Culture, and Violence, N.E. Dowd, D.G. Singer, R.F. Wilson (ed.), 2006, pp. 225–246.
[18] See on his subject: K. Jakubowicz, *Media and democracy* [in:] *Media and Democracy*, Strasbourg, Council of Europe Publication, 1998, p.14

that actions of those who try to restrict this freedom cannot be justified, because they are falsely convinced that they are infallible[19].

Article 10 of the ECHR guarantees the right to freedom of expression. The exercise of this right may, however, be subject to certain limitations for specified reasons, including the protection of health, of morals and the prevention of crime. Accordingly, freedom of expression is nowhere absolute in the European Union. Section 2 of Article 10 provides for exceptions to freedom of expression, which carries duties and responsibilities of those who want to enjoy it. This intervention must, however, be prescribed by law (and in accordance therewith[20]) and be necessary in a democratic society for safeguarding interests and rights listed in this provision. Among those considerations justifying public intervention are: prevention of disorder or crime, protection of health or morals and protection of the reputation or rights of others[21].

Balance must also be maintained between the rights of an individual and the interest of the society[22]. What is more, the State must show something more than mere « necessity » ; it should also act in good faith, with care and reasonably[23]. Even though States have a certain margin of appreciation, it is for the Court in Strasbourg to decide whether freedoms enshrined in the Convention have not been hampered with[24].

The European Court of Justice in the case of *Cinéthèque*[25] repeated that its role is also the protection of fundamental rights, including the freedom of expression - recognised throughout the EU (*via* ex Article 6 (2) TEU - also those safeguarded by the ECHR); the ECJ cannot control, however, the conformity with the ECHR of an internal act of law in the area in which Member States have unique competence. Similarly, in the morally delicate case of *Grogan*[26] *("Irish abortion case")* the ECJ reminded, that it has no jurisdiction over cases which are outside the scope of *acquis communautaire. Omega Spielhallen*[27] is one of the landmark cases on protection of human dignity in the information society. The CJEU found no violation

[19] On this subject see e.g.: A. Wiśniewski, *Znaczenie wolności słowa w państwie demokratycznym*, „Gdańskie Studia Prawnicze", 7/2000, p. 654.
[20] See for example: judgment of the European Court of Human Rights of 2 July 1984 *Malone v. UK*, A-30, p. 30.
[21] Similar regulation can be found in Articles 19 and 20 of the International Pact of Civil and Political Rights.
[22] See: opinion of 30 September 1975 on *Handyside* judgment, § 147-148.
[23] See jurisprudence of the Strasbourg Court in cases: *„Observer" and „Guardian" v. UK*, § 59 c and d; *Markt Intern Verlag GmbH and K. Beermann v. the Federal Republic of Germany*, § 33; *Weber v. Switzerland*, A-177, § 47.
[24] See: judgment of 20 May 1999 *"Bladet Tromsø" A/ Si Stensaas v. Noway*, and the report of the European commission of Human Rights of 9 July 1998.
[25] Judgment of the ECJ in the case of *Cinéthèque and others v. Fédération nationale des cinémas français*, O.J. 1985, p. 2605
[26] Judgment of the ECJ in the case C-159/90 *Society for the protection of Unborn Children v. S.Grogan and others*, O.J. 1991, p. I-4685.
[27] Case C-36/02, ECR 2004 I-09609.

of free movement of goods and freedom to provide services in German prohibition of "playing at killing" based on Article 1 of the Federal Constitution. The Court followed the argument of Advocate General Stix-Hackl and its own previous conclusions from *Schmidberger*[28], that "the Community legal order undeniably strives to ensure respect for human dignity as a general principle of law".

The US Supreme court has on many occasions ruled on possible (very limited and subject to strict tests) restrictions of the First Amendment: e.g. with respect to commercial speech in Central Hudson Gas & Electric Corp. v. Public Service Commission, 447 U.S. 557 (1980), or with respect to defamation cases as in New York Times Co. v. Sullivan.376 U.S. 254 (1964). In *Ginsberg v. New York*, 390 U.S. 629 (1968) the US Supreme Court ruled that "obscenity is not within the area of protected speech or press", citing also *Roth v. United States*, 354 U. S. 476, 354 U. S. 485. The Ginsberg ruling permitted States to regulate a minor's access to obscene material outside the presence of a parent. The fundamental reasons behind this decision were: to permit parents' claim to authority in their own household to direct the upbringing and development of their children; and secondly, to promotes the State's independent interest in helping parents protect the wellbeing of children in those instances when parents cannot be present. A three-pronged Miller test, developed by the Supreme Court in Miller v. California, 413 U.S. 15 (1973), helps define obscene speech which is not protected by the First Amendment.

5. Protection of Privacy

Professors Brandeis and Warren in their article *„The Right to Privacy"* noticed problems in defining this right, which intersects other fundamental rights and freedoms. Its most important element is the right to be let alone, which needs no further justification. Legal writing also differentiates between two aspects of privacy: vertical (individual – authorities) regulated mainly by public law; and horizontal (individual – individual) subject above all to civil law. R.A. Wasserstrom pointed out the importance of the individual's control over the flow of certain information, especially information concerning that person; whereas Barnes noticed the second side of privacy: the right not to receive unwanted information.

Article 8 ECHR provides that "everyone has the right to respect for his private and family life, his home and his correspondence «.[29]. Again, public authorities should not interfere with

[28] Case C-112/00, ECR 2003 p. I-5659.
[29] Similar provisions are contained in the Directive 95/46 of 24 October 1995 regarding data protection; O.J. 1996, L 281, p. 31, http://europa.eu.int/ISPO/legal/en/dataprot/directiv/directiv.html

this privacy for purposes other than those which are necessary in a democratic society and listed in Section 2[30]. Among those we find « prevention of disorder or crime, protection of health or morals, and protection of the rights and freedoms of others ». As in the case of applying Article 10, discussed above, fair balance must be struck between competing interests[31].

As far as new information technologies are concerned, the COE Committee of Ministers, over twenty and fifteen years ago respectively, adopted Recommendations No. R (89) 9 and No. R (95) 13, which inter alia require Member States to oblige service-providers to reveal information helping identify the user, when authorised to do so by the competent authority.

More recently, a binding instrument, i.e. the Convention on Cybercrime was passed on 23 November and entered into force on 1 July 2004. Also the UN has been concerned with the number and gravity of cyberspace crimes, adopting, among others, Resolutions 55/63 of 4 December 2000 and 56/121 of 19 December 2001. The above instruments recommend that "legal systems permit the preservation of and quick access to electronic data pertaining to particular criminal investigations". Related EU instrument is Directives 2006/24/EC, whose deadline for implementation has passed on 15 September 2007 (extended on application of 16 Member States to 15 March 2009).[32]

With respect to the above standards, we see that they give priority to the protection of victim's privacy (a frequent type of human rights violation in cyberspace) over the offender's privacy, and very rightly so. In this context, it is interesting to look at a relatively recent ECHR decision: judgement of 2 December 2008 in the case of *K.U. v. Finland*[33], where a Finnish minor (who was 12 when he fell victim to a cybercrime) was prevented by Finnish law (in force at the date of commission of a crime, though new law was in place at the time of complaint) from bringing proceedings against a person who placed an advertisement of a sexual nature on a dating site in the minor's name and without his knowledge. The Court has found a violation of art. 8 (with no need to examine the violation of art. 13 – the right to effective remedy before a national authority) ordered the respondent State to reward the minor with 3000 Euro plus any tax chargeable and interest in respect of non-pecuniary damage.

There are many views, however, especially in American doctrine, that society is "healthier" if it's based on mutual responsibility rather than confidentiality, that the world of

[30] Compare: judgment of the European Court of Human Rights of 22 October 1981 *Dudgeon v. UK*, A-45. The Court fund no premises for governmental intervention and Hus breach of Article 8 ECHR.
[31] F. Rigaux, *La protection de la vie privée et des autres biens de la personnalité*, Brussels 1990, p. 214.
[32] Implemented in Poland on 24 April 2009 (Journal of Laws No. 85, item 716) by way of amendment to Telecommunications Law, which entered into force on 1 January 2010, extending retention of data duties to all Internet providers and cable networks operators.
[33] Application no. 2872/02.

"glass houses is better than that of that of shields"[34]. The *Legal Advisory Board* of the European Commission on the other hand contends that anonymous communication is a prerequisite for freedom of communication and must be protected in the process of open political debate, however difficult it may be[35]. It must always be born in mind that also criminals operate anonymously in the Internet, and their privacy does not deserve respect.

6. European and American perspective

Digital TV, pay-per-view or near-video-on-demand services were subject to the Council of Europe *Convention on Transfrontier Television*, and within the EU – Directive 89/552 "Television without Frontiers"[36], which contained provisions safeguarding both minors and human dignity. Even though originally meant for traditional, unencrypted broadcasting services, after employing a proportionality test, the Directive had been applied to those new services. For example, Article 12 of the Directive prohibited advertising and teleshopping which could prejudice respect for human dignity. Article 16 contained explicit prohibition of certain means of advertising, based on exploitation of minors' inexperience and trust. It must be noted, that such advertisements are commonplace, so the prohibition is not reflected in practice. The entire Chapter V referred to the protection of minors and public order, prohibiting any programmes „which might seriously impair (…) development of minors (…)", requiring identification of such material by a preceding signal or accompanying visual sign. Also incitement to hatred „on grounds of race, sex, religion or nationality" must be banned by Member States.

Protection of minors (art. 12 and 13) and human dignity (art. 6) in the audiovisual sector as such is the key motivation behind the Audiovisual Media Services Directive (AMSD), replacing the abovementioned, now outdated directive[37]. It is expected to be an effective means in all EU Member States of "providing rules to shape technological developments, creating a level playing field for emerging audiovisual media, preserving cultural diversity, protecting children and consumers, safeguarding media pluralism, combating racial and religious hatred and still guaranteeing the independence of national media regulators." According to Article 12, but only with regard to non-linear audiovisual services –the Directive provides that content

[34] Por. D. Brin, *The Transparent Society*, New York 1997.
[35] LAB's response to the Green Paper; 25.02.1997. See also: "Open Internet Policy Principles adopted by the Parliamentary Human Rights Foundation", http://www.phrf.org/
[36] Directive of 3 October 1989, O.J.L 298, p. 23.
[37] Directive 2010/13/EU.

which might seriously impair minors must only be made available in such a way that ensures that minors will not normally hear or see such on-demand audiovisual media services".

A subject of a heated debate, both in Europe and the United States, are extensively violent video games. According to a Communication from the EU Commission[38] "Video games are one of the favourite leisure activities of Europeans of different ages and social categories. There are also promising opportunities for a strong interactive games industry in Europe, which is already the fastest growing and most dynamic sector in the European content industry, and has a higher growth rate than in the US, half the revenue of the music market and more than the cinema box office in Europe. The rapid growth of on-line video games is also a key driver for the uptake of broadband telecommunications networks and third generation cellular phones. All this makes video games a front-rank medium, with the result that freedom of expression for both creators and gamers is a paramount concern. However, - because of the potential psychological effects of video games on minors - this must be balanced by high standards of protection. The fact that video games are increasingly played by adults and played jointly by children and parents demands in particular differentiated levels of access to video games for minors and adults." The American judicial position in each state, despite of legislatures' efforts to protect minors, has been that of the First Amendment protection, however, on 2 November 2010 oral arguments were presented to the US Supreme Court in the case of *Schwarzenegger v. Entertainment Merchants Association et al.*[39.] The final ruling on a California ban on violent video games, introduced in 2005 and successfully challenged in the United States District Court for the Northern District of California by the industry and freedom of speech defenders was delivered in June 2011. The Court has once again elevated the 1st Amendment above any other values that could be trumped by offensive of ultra-violent modes of expression. Protection of minors was no exception, while possible violation of human dignity had – unfortunately - never been raised by California in the proceedings.

Complex EU regulation on protection of minors and human dignity in the information society is in fact in *statu nascendi*, being so far mainly soft law[40]. Previous efforts of national

[38] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the protection of consumers, in particular minors, in respect of the use of video games - 22 April 2008 - COM(2008) 207 final; following a Council Resolution on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age group, 2 March 2002 (2002/C65/02), OJ C65, 14.3.2002, p. 2.
[39] 2007 U.S. Dist. LEXIS 57472 (N.D. Cal. 2007).
[40] In accordance with the principles subsidiarity and proportionality, such non-binding (or rather – politically binding) measures are currently being promoted within the EU, which aims at de-regulation rather than strict regulation. The Parliament has already issued several resolutions touching upon the subject (see for example: Resolution of 12 October 1996, O.J. C 20, 20.1.1997, p.170; Resolution of 13 March 1997, O.J. C 115, 14.4.1997, p.151).

states and the EC itself had concentrated on traditional and from their nature centralised mass media, in particular television. The key document which started the debate is the Commission Green Paper of 16 October 1996[41], followed by consultations and the Council Recommendation 98/560 of 24 September 1998[42]. A parallel Commission document was the Communication on Illegal Content on the Internet[43], together with the Parliament Resolution which called on the Commission to draw up a European quality rating system for providers of Internet services and to support international coordination of such ratings and to propose a common framework for self-regulation at EU level; and asked the Member States to define a minimum number of common rules in their criminal law. The European Parliament and the Council also issued a Decision (No 276/1999/EC) adopting the first multi-annual (1999-2002) Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks[44]. On 30 April 2004, a proposal was drafted for a Recommendation on the protection of minors and human dignity and the right of reply in relation to the competitiveness of the European audiovisual and information services industry[45]. Here, another type of information services was noticed, namely 3-G mobile phones, which convey audiovisual content, and will soon become particularly attractive to children.

Besides the comparative analysis of national criminal law solutions concerning illicit (legal, but capable of being harmful to minors) or illegal content and constitutional protection of the freedom of expression, the importance of balancing fundamental rights is being stressed in relevant documents. Particular attention is brought to Articles 8 and 10 ECHR, which may only be restricted if they are prescribed by law (and in accordance with law), necessary in a democratic society for the objective to be attained, and proportional. On the other hand, there is a need for a "common indicative framework" pointing at rules which are technically and economically feasible and guarantee the development of the single internal market and the information society in Europe, but also the protection of fundamental values.

A Declaration on freedom of communication on the Internet was adopted by the Council of Europe on 23 May 2003, which contained rules such as: promoting self-regulation and co-regulation, absence of prior state control of content presented in the Internet (with the exception of filters for the protection of minors), removal of such content only after provisional or final decision on its illegality has been taken by competent authorities, anonymity (with the

[41] COM(96) 483 final.
[42] O.J.1998, L 270, p. 48
[43] COM(96)48.
[44] O.J. 1999, L 33, p. 1.
[45] COM(2004)341 final.

exception of tracing criminals), due care for the freedom of expression and limited liability of service providers. In its preamble, the Declaration stipulates that "freedom of communication on the Internet should not prejudice the human dignity, human rights and fundamental freedoms of others; especially minors".

Among the proposals formulated by respondents to Commission Communications was the creation of EU legislation and specific codes of conduct (mainly self-regulatory, introduced by the industry itself and based mainly on rating and classification of audiovisual content) and a body responsible for its implementation and control of national activities. Not only the industry, but also the family should, according to those contributions, be embarked with responsibility; and the Member States should encourage parental control and create respective legal background. As a result, we now observe the abundance of initiatives by major content and service providers, with notable results such as the CEO Coalition to make the Internet a better place for kids, launched in December 2011, the European Framework for Safer Mobile Use by Younger Teenagers and Children of February 2007 with related national codes of conduct, or the Safer Social Networking Principles for the EU of 10 February 2009. The above documents share responsibility among all stakeholders: the industry, parents and teachers, governments and law enforcement bodies, but also the users themselves. Multi-stakeholder collaboration indeed may be the most effective way to protect minors and human dignity, as long as it does not release from liability and responsibility those who profit economically from the respective business, ignoring potential infringements. Similarly, the recent Commission Recommendation on on-line gambling of 14 July 2014[46], aims at protecting minors by putting forward information duties preventing minors from access and restrictions on advertising, which with Member States' voluntary regulation will hopefully be observed by service providers.

7. Concluding remarks

Despite many advantages of the information society era, legislators have to be prepared to face new challenges every day. Judges, in turn, must be able to balance contradictory interests of individuals, the society as a whole and the State as such. In some cases, self-regulation can turn out to be the most effective means of protecting overriding values, such as human dignity and the integrity of children. In respect of the latter, the role of parents cannot be overestimated.

[46] C (2014) 4630/3.

It goes without saying that nowadays only combination of all the above means, will result in a desirable level of protection of minors and human dignity.

Part 3

Challenges of IP and Data protection

Chapter 1

THE CLASH BETWEEN PROTECTION OF PERSONAL DATA AND PROTECTION OF INTELLECTUAL PROPERTY RIGHTS IN INTERNET IN THE CJEU JURISPRUDENCE

Krystyna Kowalik-Bańczyk

Associate Professor, Institute of Legal Studies, Polish Academy of Sciences, Chair of Competition Law, 72 Nowy Świat, 00-330 Warszawa, Poland, kkowalik@inp.pan.pl

Keywords: *Personal data protection, intellectual property, Court of Justice of European Union*

Abstract*: The aim of the research is to identify what result brings the balancing between the protection of personal data and the protection of intellectual property rights undertaken by the Court of Justice of the European Union (CJEU) in its recent jurisprudence. The research should explain three main questions: first, why the Internet Protocol (IP) addresses belong to the personal data. Second, if it would be legitimate to place the liability for identifying and blocking the IPR infringements on the internet service providers only Third, what is the rationale for the position of the CJEU not to accept such claims of IPR holders. The author searches to find out whether the CJEU jurisprudence indicates that there is a certain hierarchy between data protection and IPR protection.*

The aim of this paper is to identify what result brings the balancing between the protection of personal data and the protection of intellectual property rights undertaken by the Court of Justice of the European Union (CJEU) in its jurisprudence on the legal acts aimed at regulating the activities in the Internet. It is obvious to state that the Internet eases and speeds up all possible infringements of intellectual property rights (IPR). In this context, the CJEU is often asked to judge the lawfulness of requirement of IPR holders directed to internet service providers (ISP) to introduce some systems for monitoring and filtering of their customers' Internet usage in order to block the transfer of files containing IPR rights and to identify the customers that commit infringements. In this text, the focus should be put on three main questions: first, what data on the customers belong to the personal data within the meaning of

Directive 95/46[1], and particularly, if IP addresses always constitute personal data. Second, it is analysed if it would be legitimate to place the liability for identifying and blocking the IPR infringements on the internet service providers. For any plaintiff alleging IPR infringement both questions – of identification and of blockade - are important. The IPR holder might seek to identify the primary infringer and then to prevent ISP from future repetition of any such situation of infringement[2]. It is however adding a new burden to the obligations of ISP. Third, the paper should search what is the rationale for the position of the CJEU not to accept such claims of IPR holders to either deliver information of infringer or to monitor the content of the services online. There are however examples of judgments where the CJEU simply imposes on IPRs an obligation to block the access to the infringing content[3]. The text aims to find out whether the CJEU jurisprudence indicates that there is a certain hierarchy between data protection and IPR protection, with some primacy given to the personal data protection issues. By this the CJEU is reducing the legal protection of IPR rights holders and granting an (excessive?) protection to those who access the infringing content on-line. This tendency is also reflected in the solutions of Polish law that are broadly analysed elsewhere[4].

1. The IP addresses as personal data

In order to identify the alleged infringer, the ISPs are often requested to reveal the information on the IP address of the computer used to post infringing materials. They usually refuse due to the argument that the questioned information covers personal data. Personal data are understood as data that allow for identification of a particular person[5]. The problem if IP address really allows for identification raised litigation in different national courts[6], because of the unclear definition of "personal data"[7]. There is at present no doubt that the IP addresses

[1] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50.
[2] A. Savin, *EU Internet Law*, Cheltenham, Northampton 2013, p. 119.
[3] CJEU judgment of 27.03.2014 in case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192.
[4] P. Litwiński, *Anonimowość w sieci. Zagadnienia udostępniania danych osobowych* [in:] *Internet. Prawo-informatyczne problemy sieci, portali i e-usług*, G. Szpor, W. Wiewiórowski (eds.), Warszawa 2012, p. 217-226, particularly on previously existing art. 29 of the Law on protection of personal data and the jurisprudence related to it and the changes of law in 2010.
[5] On a difference between "data" and „information" – cf W. Wiewiórowski, *Ponowne przetwarzanie informacji publicznej zawierającej dane osobowe* [in:] *Główne problemy prawa do informacji*, G. Sibiga (ed.),Warszawa 2013, p. 393.
[6] Described broader in: K. Klafkowska-Waśniowska, *Commentary to art. 18* [in:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, M. Namysłowska, D. Lubasz (eds.),Warszawa 2011, p. 276-277.
[7] L. Bygrave, *Data Privacy Law. An International Perspective*, Oxford 2014, p. 137.

personal data[8], especially in the ISP systems where the user has to log in[9]. In this way the ISP is in possession of broader picture of a person using a service than just an IP address that is helping to localize the user[10] and could easily identify them. The IP address is not a personal data only when it does not allow to identify the user[11] (f.i. IP of a library or internet café[12]).

The CJEU has held for several times that IP addresses are personal data, not even making the above clarification given by the Article 29 Working Party as to the various characters of IP addresses. The case C-275/06 *Productores de Música de España (Promusicae)*[13] of 2008 was the first judgment where the CJEU clearly underlined that the IP addresses should be covered by the confidentiality principle of electronic communication in the context of balancing the individual right to privacy with the protection of IPR rights. In this case the Telefónica refused to disclose to Promusicae personal data relating to use of the internet by means of connections provided by Telefónica. According to Promusicae several customers of Telefónica used the KaZaA file exchange program and provided access to shared files of personal computers to phonograms covered by IPR rights' of Promusicae members. The CJEU in this case considered that the personal data (like IP addresses) must be protected and that it would be unproportioned to disclose them every time the IPR rights are infringed. Thus the national authorities were asked to provide for a fair balance between the two protected values[14]. In this case an important distinction as to the scope of ISP obligations was made. The CJEU underlined that the IP addresses should be delivered by intermediaries (ISP) in criminal proceedings but this obligation does not occur in any other (mainly civil or administrative) proceedings[15]. Thus, the

[8] The notion of personal data itself has been interpreter by the CJEU – cf judgment of 6.11.2003 in case C-101/01 *Lindqvist*, ECLI:EU:C:2003:596, para 24: "The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies".

[9] J. Gołaczyński, *Commentary to art. 16* [in:] *Ustawa o świadczeniu usług drogą elektroniczną*. Komentarz, J. Gołaczyński (ed.), Warszawa 2009, p. 140.

[10] K. Klafkowska-Waśniowska, *Commentary to art. 18* [in:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, M. Namysłowska, D. Lubasz (eds.), Warszawa 2011, p. 268.

[11] Opinion 4/2007 on the concept of personal data, of 20 June 2007, 01248/07/PL WP 136, Article 29 Data Protection Working Party, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (accessed February 2014), p. 16-17.

[12] But even such data, when brought in relation to other information (time, register of users etc) might be a personal data, cf Opinion 4/2007 on the concept of personal data, of 20 June 2007, 01248/07/PL WP 136, Article 29 Data Protection Working Party, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf (accessed February 2014), p. 11, 17.

[13] CJEU judgment of 29.01.2008 in case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54, para 45. Cf A. Savin, *EU Internet Law*…, p. 146.

[14] CJEU judgment of 29.01.2008 in case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54, para 70.

[15] P. Polański, *Prawo Internetu*, Warszawa 2014, p. XVII.

protection of personal data might differ in different Member States, depending on the legislative choices made by the national Parliaments as to the legal qualification of IPR infringements. Yet, the harmonization introduced by most of the directives on protection of IPR rights in Internet do not leave the Member States so much freedom of action and such legislative choices. The directives do not allow Member States to protect authors in a broader way than the directives themselves[16].

The *Scarlet Extended*[17] case was based on the preliminary reference in the proceedings between Scarlet Extended SA and the Société belge des auteurs, compositeurs et éditeurs (SABAM) concerning Scarlet's refusal to install a system for filtering electronic communications with use file-sharing software (so called peer-to-peer) in order to prevent file sharing that could infringe copyright. Scarlet Extended was a typical ISP, providing its customers with access to internet but without offering other services like file sharing or downloading. Its services were used by internet users to create peer-to-peer networks as a method of file sharing. The Belgian court imposed on Scarlet an injunction to bring an end to this copyright infringement by making it impossible for customers to send and receive files containing musical work in SABAM's repertoire. Scarlet raised that the installation of a filtering system would be in breach of the provisions of EU law on the protection of personal data because filtering would imply processing of IP addresses that are personal data. CJEU admitted that such an injunction would impose on ISP concerned an obligation to actively monitor all the data relating to each of its customers, which is prohibited by art. 15 of the e-commerce directive[18].

Similarly, in case *Bonnier Audio*[19] the applicants in the Swedish proceedings were publishing companies which hold exclusive rights to reproduction, publishing and distribution of 27 works in form of audio books. Those books were publicly distributed without their consent by file transfer protocol which took place thanks to internet service provider called ePhone. The applicants asked ePhone to disclose the date of person using an IP address from which the files in question were sent on a particular date. CJEU stated that the communication sought by applicants constitutes a processing of personal data within the meaning of art. 2 of

[16] CJEU judgment of 13.02.2014 in case C-466/12 *Nils Svensson et al. v Retriever Sverige AB*, ECLI:EU:C:2014:76.
[17] CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771.
[18] CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 40.
[19] CJEU judgment of 19.04.2012 in case C-461/10 *Bonnier Audio AB, Earbooks AB et al v Perfect Communication Sweden AB*, ECLI:EU:C:2012:219.

Directive 2002/58 read in conjunction with art. 2 (b) of Directive 95/46[20]. Any installation of filtering system by ISP would "*involve a systematic analysis of all content and the collection and identification of users' IP addresses*"[21]. The IP addresses are protected personal data, because they allow to precisely identify the users. Thus fundamental rights of customers of ISP would be regularly infringed[22]. This exclusion of general monitoring is confirmed in the case *SABAM v Netlog NV*[23].

It is visible that in the above jurisprudence of CJEU that the distinction "criminal proceedings versus other kinds of proceedings" are not so much underlined, it is rather the question of scope of actions for identifying either a particular infringer or all infringers. Lee Bygrave notes that all those decisions are '*cursory and fail to clearly distinguish the status of IP address vis-à-vis IPR holders and their status vis-à-vis ISPs*'[24]. Some liability is placed on ISP but its scope remains uncertain.

2. Placing the liability for identifying and blocking the IPR infringements on the internet service providers

In the structure of Internet there are always three categories of subjects: those who create or post information, those who are targeted by that information (recipients, customers) and those who permit for exchange of information – namely the intermediaries (ISP)[25]. The intermediaries are "*an inevitable actor in any transmission of an infringement over the internet between one of its customers and a third party, since, in granting access to the network, it makes that transmission possible*"[26]. If the intermediaries are "discouraged" by the legislator to act freely by imposing on them liabilities for the content or behaviors of subjects from the first or second categories, they might be less willing to undertake such intermediary activities and further develop Internet. Because of this relationship, noted by different authors[27], the European

[20] CJEU judgment of 19 April 2012 in case C-461/10 *Bonnier Audio AB, Earbooks AB et al v Perfect Communication Sweden AB*, para 52.
[21] CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 51.
[22] Not only their right to protection of personal data but also their right to receive and impart information, CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 50, 51.
[23] CJEU judgment of 16.02.2012 in case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, ECLI:EU:C:2012:85.
[24] L. Bygrave, *Data Privacy Law…*, p. 138.
[25] A. Savin, *EU Internet Law*..., p. 104.
[26] CJEU judgment of 27.03.2014 in case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192, para 32 ; CJEU order in case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, ECLI:EU:C:2009:107, para 44.
[27] Signalling such a relationship - A. Savin, *EU Internet Law…*, p. 105.

model of business activities for intermediaries, set in e-commerce directive[28], steers into direction of exempting them from too many obligations and liabilities that might be discouraging to them. In the preamble of directive 2000/31 in point 47 it is clearly stated that "*Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of general nature*". Also article 15 of the same directive states that "*1. Member States shall not impose a general obligation on providers, when providing the services covered by Art. 12, 13 and 14 to monitor the information, which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating unlawful activity*". On the other hand, the individual injunctions against intermediaries whose services are being used by a third party to infringe the right holder's intellectual property rights are allowed both by the Directive 2001/29[29] (art. 8.3)[30] and Directive 2004/48[31] (art. 11). Still, as the name signals, the intermediaries are just intermediaries and are not willing to engage in disputes between the content providers and recipients. The burden placed on them to monitor content in their servers might amount to self-censorship in order to avoid liability. Therefore some countries opt for granting the ISP for complete immunity (like USA[32]) or limiting that liability on the condition that any infringing material should be removed upon notification[33], like in the European Union[34] (as the above cases indicate).

Despite the general European trend to "spare" the ISP, the CJEU has applied art. 8 (3) of the Directive 2004/48 to state that this provision does not preclude Member States from imposing an obligation to disclose to private person's personal data in order to enable them to bring civil proceedings for copyright infringements. However the Member States are not obliged to lay such obligations[35] and they must not take such an interpretation of this provision

[28] P. Polański, *Odpowiedzialność prawna za treści rozpowszechniane w Internecie/Legal liability for content disseminated over the Internet*, Warszawa 2012, available at: http://www.natolin.edu.pl/pdf/zeszyty/Natolin_Zeszty_48.pdf (accessed February 2015).
[29] Directive 2001/29/EC of the European Parliament and of the Council of 22.05.2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10-19.
[30] Cf CJEU judgment of 27.03.2014 in case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft*, ECLI:EU:C:2014:192.
[31] Directive 2004/48/EC of the European Parliament and of the Council of 29.04.2004 on the enforcement of intellectual property rights, OJ L 157, 30.4.2004, p. 45–86.
[32] Section 230 of the Communication Decency Act 1996 (liability of intermediaries in general) and Section 512 of Digital Millenium Copyright Act 1998 (liability of intermediaries for copyright infringements).
[33] Signalling such a relationship - A. Savin, *EU Internet Law…*, p. 108.
[34] Cf CJEU judgment of 12.07.2011 in case C-324/09 *L'Oréal SA, Lancôme parfums and beauté et al v eBay International*, ECLI:EU:C:2011:474.
[35] CJEU judgment of 29.01.2008 in case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54, para 54, 55; CJEU order in case C-557/07 *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, ECLI:EU:C:2009:107, para 29; CJEU judgment of 19.04.2012 in case C-461/10 *Bonnier Audio AB, Earbooks AB et al v Perfect Communication Sweden AB*, ECLI:EU:C:2012:219, para 55.

that would conflict with the fundamental rights or general principles of EU law (mainly the principle of proportionality)[36]. On the other hand, it also occurred that the CJEU was asked to judge the lawfulness of requirement of IPR holders to ISP to introduce a system for systematically monitoring and filtering of its customers' Internet usage in order to block the transfer of files containing IPR rights. As the IPR holders required it for an unlimited period of time and at the cost of ISP, the CJEU found it not proportional[37].

In the already cited case *SABAM v Netlog NV*[38] concerning proceedings between SABAM and the owner of an online social networking platform Netlog, in which SABAM was trying to oblige Netlog to introduce a system for filtering information stored on its platform, the CJEU excluded yet again the possibility to introduce a general monitoring system, because it would breach the art. 15 (1) of the directive 2000/31[39] and art. 3 of the directive 2004/48[40]. Such a solution of systematic monitoring could infringe not only the protection of personal data[41], but also it could undermine the freedom to information as the system would not be able to distinguish between unlawful and lawful content and might lead to blocking the lawful communications[42].

On the other hand, in the case C-314/12 *UPC Telekabel*[43], the internet site under domain "kino.to" that allowed its users to access the films protected by copyright, the CJEU confirmed that the ISP might be obliged to block access to this webpage because it allowed for copyright infringements. It is however a solution that block the infringement and does not include any problems of personal data protection.

---

[36] CJEU judgment of 19.04.2012 in case C-461/10 *Bonnier Audio AB, Earbooks AB et al v Perfect Communication Sweden AB*, ECLI:EU:C:2012:219, para 56. Such argumentation was even named in the literature "constitutionalisation" of IPR – cf C. Geiger, *"Constitutionalizing" Intellectual Property Law? The Influence of Fundamental Rights on Itellectual Property in the European Union?* "International Review of Intellectual Property and Competition Law" 2006/37, p. 371.

[37] L. Bygrave, *Data Privacy Law…*, p. 149.

[38] CJEU judgment of 16.02.2012 in case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, ECLI:EU:C:2012:85.

[39] CJEU judgment of 16.02.2012 in case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, ECLI:EU:C:2012:85, para 33.

[40] CJEU judgment of 16.02.2012 in case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, ECLI:EU:C:2012:85, para 34.

[41] CJEU judgment of 16.02.2012 in case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, ECLI:EU:C:2012:85, para 49.

[42] CJEU judgment of 16.02.2012 in case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, ECLI:EU:C:2012:85, para 50.

[43] CJEU judgment of 27.03.2014 in case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192.

3. The rationale for not accepting the IPR holders claims to reveal personal data

The main reasons for not accepting the IPR holders' claims is their try to impose an *ex ante control* of content presented on ISP servers. Any general measures on preventive control are excluded by the secondary law of the EU Internet directives. The reasons for not agreeing on such preventive measures might be that they clash with three main values: the right to protection of personal data or the freedom to receive or impart information[44] enjoyed by the users and the freedom to conduct business, enjoyed by the ISP. Thus it is visible that two different groups of the above mentioned triangle: IPR holders, users and ISPs – are protected.

If we want to protect the customers or users (being in fact often also the infringers of IPR rights), there are several references to the issue of personal data protection. The scope of this protection is extending beyond the issues analyzed in this paper[45]. In particular, the question of users' right to protect their personal data is raised, as possibly violating not only provisions of secondary EU law on data protection (mainly the directive 95/45 and directive 2002/58) but possibly also art. 8 of the Charter of Fundamental Rights of the European Union. There is as well appearing an argument of the protection of freedom to information, that might undergo serious limitations in case of any structural "filtering" of the content transmitted by the ISPs. The cases *Scarlet v Sabam* and *Scarlet v Netlog* illustrate well the clash between the copyright protection and freedom of expression[46]. This argument was also raised in *UPC Telekabel*, where the CJEU stated that any injunction to block access to content infringing IPR rights must be formulated with respect to the balance between IPR protection and both freedom to conduct a business (art. 16 of the Charter of Fundamental Rights) and freedom of information of internet users (art. 11 of the Charter)[47].

Both of those arguments referring to the protection of Internet users appeared in the case C-70/10 *Scarlet Extended SA p. Société belge des auteurs, compositeurs et éditeurs (SABAM)*. The CJEU stated that consequences of such system of filtering of content, if such a system was imposed on an ISP, would not limit themselves to this ISP concerned. The filtering system is by definition infringing the fundamental rights of customers of such an ISP – both their personal

[44] CJEU judgment of 16.02.2012 in case C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, ECLI:EU:C:2012:85, para 51, CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 53.
[45] Cf CJEU judgment of 11.12.2014 in case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428.
[46] S. Kulk, F. Borgesius, *Filtering for Copyright Enforcement in Europe after the SABAM cases*, "European Intellectual Property Review" 2012/11, p. 791-795.
[47] CJEU judgment of 27.03.2014 in case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192, para 47.

data protection rights and their freedom to receive and transmit information. Thus such a system would infringe both art. 8 and art. 11 of the Charter[48]. A relationship between those values – the freedom of information and protection of personal data, has been analysed by the CJEU in case C-73/07 *Satakunnan et Satamedia*[49]. The case appeared in a dispute between the data protection authority and two Finnish companies - Satakunnan Markkinapörssi Oy i Satamedia Oy. One of those companies was legally receiving available personal data from tax authorities and publishing them in a journal called Veropörssi. About 1,2 million persons' personal data, including their income, once that income was of certain value, were published in alphabetical order, with an estimated information on the level of taxes that they pay. Markkinapörssi allowed its share-holder, company Satamedia, to use the personal data published in Veropörssi and to both publish them in form of CDRoms and allowing for distribution of information upon request by SMS. Both companies concluded a contract with a telecom company to provide them with a SMS service allowing the mobile phone owners to obtain SEMes (for 2 euro per SMS) with information published in *Veropörssi.* The CJEU had not doubt that the data transmitted are personal data, however because they were anyway publicly available, no infringement was stated – and this was enhanced by the fact, that otherwise freedom to obtain information could have been limited.

In *Bonnier Audio* CJEU listed the conditions that need to be fulfilled in order to ensure that the fair balance is stuck between the protection of IPR rights and protection of personal data enjoyed by internet subscribers or users. The legislation such as Swedish legislation in case, should thus:

- require that, for an order for disclosure of data in question to be made, there is clear evidence of an infringement of IPR;
- the required information can be regarded as facilitating the investigation into an infringement of copyright or impairment of that right;
- reasons for the measure (disclosure of personal data) outweigh the nuisance or other harm which the measure might entail for the person affected by it or some other conflicting interest[50].

[48] CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 50.
[49] CJEU judgment of 16.12.2008 in case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, ECLI:EU:C:2008:727.
[50] CJEU judgment of 19.04.2012 in case C-461/10 *Bonnier Audio AB, Earbooks AB et al v Perfect Communication Sweden AB*, ECLI:EU:C:2012:219, paras 58-60.

On the other hand, if we want to protect the ISPs, the main argument remains their freedom to conduct business. The eventual limitations to filter content, imposed on them, is often judged by CJEU as too burdensome and thus not fulfilling the requirements of the principle of proportionality. A try to impose a system of control for the provider of an online social networking service – like in the case *Scarlet Extended* – has been judged by the CJEU as the case based on proportionality principle. The cases where the ISP were ordered to exclude (block) access to the content infringing IPRs without any clear obligation to monitor the content – do happen, however with a clear obligation to respect both the freedom to conduct business and the freedom of information[51].

4. Conclusion – a hierarchy between data protection and IPR protection

Since *Promusicae* case of 2008, the CJEU underlines that the protection of IPR must be balanced against the protection of other fundamental rights[52]. In *Scarlet Extended* CJEU clearly stated that "*protection of the right to intellectual property is indeed enshrined in Article 17(2) of the Charter of Fundamental Rights of the European Union. There is, however, nothing whatsoever in the wording of that provision or in the Court's case-law to suggest that that right is inviolable and must for that reason be absolutely protected*"[53]. The reasons for setting aside the protection of IPR might be protection of freedom to conduct a business (pursuant to art. 16 of the Charter)[54] or protection of privacy and freedom to receive information (art. 8 and 11 of the Charter)[55]. The presented cases allow the author to presume that the balancing between the protection of personal data and the IPR protection favours the protection of individual right to privacy and personal data protection in detriment to the IPR holders.

Thus one corner of the above mentioned triangle consisting of content providers – intermediaries (ISP) and – users, is clearly privileged. Whereas the ISP are feeling a growing burden of responsibility to avoid infringements of IPS rights, the Internet users that are committing those infringements are usually impossible to identify. With the growing CJEU caselaw on personal data and privacy protection[56], the Internet users are most probably bound

[51] CJEU judgment of 27.03.2014 in case C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*, ECLI:EU:C:2014:192, para 47, 63.
[52] CJEU judgment of 29.01.2008 in case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECLI:EU:C:2008:54, paras 62-68.
[53] CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 43.
[54] CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 46.
[55] CJEU judgment of 24.11.2011 in case C-70/10 *Scarlet Extended v SABAM*, ECLI:EU:C:2011:771, para 50.
[56] CJEU judgment of 13.05.2014 in case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, not yet reported, ECLI:EU:C:2014:317; CJEU judgment of 04.2014 in joint cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The*

to be left free of liability. It is the relationship between ISP and content providers where the main struggle to protect IPR rights will be continued.

Commissioner of the Garda Síochána, Ireland and the Attorney General; and KärntnerLandesregierung, Michael Seitlinger, ChristofTschohl and Others, not yet reported, ECLI:EU:C:2014:238; CJEU judgment of 11.12.2014 in case C-212/13 *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, not yet reported, ECLI:EU:C:2014:2428.

Chapter 2

WRONG ASSUMPTIONS, WRONG CONCLUSIONS. ECONOMICS OF INTANGIBLE GOODS AND ITS IMPACT ON INTERPRETATIONS OF COPYRIGHT LAW ON THE INTERNET

Konrad Gliściński

Ph.D Candidate, Jagiellonian University, Faculty of Law and Administration, ul. Gołębia 24, 31-007 Kraków, Kalecki Foundation associate, kgliscinski@gmail.com

Keywords: *copyright, public goods, Case C 435/12, InfoSoc Directive (2001/29/EC), piracy*

Abstract:

If you make a wrong assumption, you come to wrong conclusion.

Michał Kalecki

1. Introduction - What have we learned?

The use of new media by scientific institutions, new strategies for the collection, transfer and acquisition of knowledge, the availability of e-book readers, the use of cyberspace in contemporary artistic forms, the use of elements of digital culture in contemporary art ─ everything that is technically possible, but very often it is impossible or difficult for legal reasons.

Although this is a trivial one must admit that at the time when the InfoSoc Directive (2001/29/EC) was created knowledge about functioning of the Internet differed significantly from the knowledge that we have today. Wrong assumptions used during its creation, unfortunately, also affect the current interpretation thereof. Some of these wrong assumptions results from a general misunderstanding of the principles of operation of intangible assets (e.g. works). Currently functioning model of copyright is based on assumptions derived from the operation of the economy of material goods. For obvious reasons, this article only at the basic level indicates the scheme of considerations that should be applied in the interpretation of laws

relating to intangible goods. Only on this background it is possible to provide a correct interpretation of the exceptions and limitations of European copyright law.

2. Wrong assumptions[1]

Assumption No.1: Illegal forms of distribution of counterfeited or pirated works are always wrong to support the dissemination of culture

(recital 22) The objective of proper support for the dissemination of culture must not be achieved by sacrificing strict protection of rights or by tolerating illegal forms of distribution of counterfeited or pirated works.

Assumption No.2: Private use cause the prejudice to rightholders and digital private copying has a greater negative economic impact on the rightholders than analogue private copying

(recital 35) When determining (...) possible level of such fair compensation, account should be taken of the particular circumstances of each case. When evaluating these circumstances, a valuable criterion would be the possible harm to the rightholders resulting from the act in question. (recital 38) Digital private copying is likely to be more widespread and have a greater economic impact.

Assumption No.3: Intangible goods should be treated as tangible goods that is, they should be (in each case) protected by exclusive rights

(recital 25) It should be made clear that all rightholders recognised by this Directive should have an exclusive right to make available to the public copyright works or any other subject-matter (...)

Assumption No.4: Interests of authors are the same as interests of others rightholders

This is an implied assumption, resulting from the use of the single term rightholder.

3. Wrong conclusions[2]

Acceptance of wrong assumptions must lead to wrong conclusions. The main question in the case C 435/12 was whether EU law, in particular Article 5(2)(b) of Directive 2001/29, read in conjunction with paragraph 5 of that article, is to be interpreted as precluding national legislation, which does not distinguish the situation in which the source from which a reproduction for private use is made is lawful from that in which that source is unlawful and,

[1] Assumptions, and the corresponding "recital" are derived from the Directive 2001/29/EC.
[2] Conclusions, and the corresponding "paragraphs" comes form of the judgement (Case C 435/12).

furthermore, whether the private copying levy may be calculated and charged only by reference to reproductions made from lawful sources. The court responded positively to these questions.

Conclusion No.1: Person who has made the copy of the protected work without seeking prior authorization from the rightholder caused damages which has to be compensated

(paragraph 39) reproductions may be made from an unlawful source would encourage the circulation of counterfeited or pirated works, thus inevitably reducing the volume of sales or of other lawful transactions relating to the protected works, with the result that a normal exploitation of those works would be adversely affected. (paragraph 40) (...) the application of such national legislation (which makes no distinction between the lawful or unlawful nature of the source. K.G.) may having (...) unreasonably prejudice copyright holders. (paragraph 50) The purpose of such compensation (private copying levy. K.G.) is, according to the case-law of the Court, to compensate authors for private copies made of their protected works without their authorisation, with the result that it must be regarded as recompense for the harm suffered by authors as a result of such unauthorised copies.

Conclusion No.2: National legislation has to make distinction between private copies made from lawful sources and those made from counterfeited or pirated sources.

(paragraph 36) the objective of proper support for the dissemination of culture must not be achieved by sacrificing strict protection of rights or by tolerating illegal forms of distribution of counterfeited or pirated works. (paragraph 37) Consequently, national legislation which makes no distinction between private copies made from lawful sources and those made from counterfeited or pirated sources cannot be tolerated.

4. What is wrong with these assumptions*?*

4.1. Illegal forms of distribution of counterfeited or pirated works are always wrong to support the dissemination of culture?

No piracy, no Enlightenment!

The phenomenon of so-called piracy, that is illegal reprinting of protected books, appeared in reaction to the first printing privileges, which then transformed into a copyright. This resulted from two interrelated reasons. Printing privileges serve as an instrument of censorship (state and church). Illegal copies (i.e. copies issued without obtaining appropriate authorization, or in violation of an existing privilege) allowed people to read the texts, recognized by the church or the state authorities as wrong, heretical or dangerous. People from the Renaissance period wanted to learn new things. It did not matter to them whether or not a book is or is not covered by the applicable privilege. Thirst for knowledge made the demand

for books. It was clear that the printers who acted legally could not provide all the required books. In this situation, the only solution were illegal printers. Over time, there has been the formation of the book market, where there were two business models that allow readers access to books. One of them was based on the monopoly of copyright. Printer produces a limited number of books and sells them at a high price. To get his monopoly prices, he has to restrict production. It was he who bears the cost of purchasing the manuscript. The second model, in turn, was based on the maximum use, in all possible ways, of freedom of printing and reprinting of books. In this way it was possible to provide for a larger number of readers' access to books at lower prices. Both models ensure implementations of different social goals, while providing adequate profits for themselves.

Of course, between these two models there was a real competitive war. It is not surprising that disputes between them often were placed in courts. These disputes in fact aimed at securing (through legal means) a greater share of profits from the book market. For the same reasons lobbying activities was undertaken. "The real key to success is to make sure that there won't ever be competition – or at least there won't be competition for a long enough time that one can make a monopoly killing in the meanwhile. The simplest way to a suitable monopoly is getting the government to give you one"[3]. An example of such legal monopoly are the *privileges* and *copyright* which are based on the *right of exclusivity*.

Adrian Johns, in his extensive monograph on piracy, clearly pointed out how the phenomenon of illegal reprints assisted in the implementation of the main goal the Age of Enlightenment which was to spread knowledge:

"Printed ideas attained ubiquity not only by distribution from major centers, but also by tension and competition between them and a more numerous set of reprinters, who acted as relays between author and reader. The more the competition, the greater the ubiquity. Locke's works, for example, emerged first from London, but were reprinted in Dublin, Glasgow, Amsterdam, The Hague, Rotterdam, Geneva, Brussels, Paris, Leipzig, Uppsala, Jena, Mannheim, Milan, Naples, Stockholm (by order of the Swedish Riksdag, no less), and, ultimately, Boston (…). Goethe's *Sorrows of Young Werther,* probably the most sensational single publishing phenomenon of the century, achieved that status by virtue of appearing in some thirty different editions, many of them in translation, and almost all unauthorized. (…) Knowledge therefore spread through chain reactions of reappropriations, generally unauthorized and often denounced (…) An initial edition from one location would find its way

[3] J. E. Stiglitz, *The price of inequality*, London 2012, p. 53.

to a place of reprinting, which would generate a thousand new copies; one of those would then spark another explosion of copies from another reprint center; and so on. Enlightenment traveled atop a cascade of reprints. No piracy, we might say, no Enlightenment"[4].

Copyright was and remains a mechanism which skillful use of can provide citizens with an optimal level of access to the works. An example of such thinking is the history of the operation of the law in the United States in the nineteenth century. In accordance with it the benefits of the copyright could be entitled only to US citizens[5]. For this reason, the vast majority of books published in the UK could not be so protected in America. As a result of which American publishers can freely print and sell this kinds of books. This state of affairs was not any accidental gap in the law, which was created by the omission of the legislators. This solution was an expression of deliberate policy of the newly formed country. "At this time (…) is fair to say that US policy reflected the utilitarian justification of the public interest"[6]. For that reason, import, sale and reprint of books written by authors who did not have US citizenship was recognized as completely legal[7]. Putting the interests of American citizens over the lamentations of publishers from abroad, the American authorities simply gave the home publishers specific state aid. As a result of this the principle of wide access to cheap books policy has been introduced, which became an important element of the mass public education[8]. The same thing happened in the case of musical creation[9]. As a result of deliberate action by the US authorities gigantic literary and scientific achievements found in the public domain, making it available to the broad masses of the nascent American society[10].

4.2. Interests of authors are the same as interests of others rightholders?

In Art. 13 of the TRIPS Agreement, which governs the three-step test, the term *interest of the author* (derived from the Berne Convention) has been replaced by the new term that is *interests of the right holder*. A similar terminological convention was adopted also in the field of European law, including the text of the InfoSoc Directive and the judgment in Case C 435/12. The use of the term *rightholders* blurs the picture of the actual mosaic of interests which clash under copyright law. Under copyright law, there are at least three groups of actors who have

[4] A. Johns, *Piracy. The intellectual property wars from Gutenberg to Gates*, Chicago-London, 2009, p. 50
[5] B. Balazs, *Coda: A Short History of Book Piracy* [in:] *Media Piracy in Emerging Economies*, J. Karaganis (ed.) Social Science Research Council 2011, p. 408.
[6] Ch. May, S.K. Sell, *Intellectual property rights. A critical history*, London 2006, p. 114.
[7] See sec. 5 of Copyright Act of 1790 http://www.copyright.gov/history/1790act.pdf (access 22.06.2014).
[8] B. Balazs, *Coda: A Short History…*, p. 408.
[9] R. Garofalo, *From Music Publishing to MP3: Music and Industry in the Twentieth Century*, American Music 1999/3, p. 321.
[10] D. Saunders, *Authorship and copyright*, London 1992, p. 156.

their own interests. These are: *Authors*, *Other Citizens (Public Interest) and Copyright Management Entities (publisher, producers, etc.)*. The obvious interest of citizens is to obtain access to the optimal number of new and old works at the lowest possible cost. The main interest of the authors is to ensure the wide distribution of their works and receive appropriate remuneration. Fundamental interest of other rightholders is related to the possession of a right that allows them to block competitors.

Copyright is trying to balance these different interests. It is therefore necessary to answer the basic question of whether: 1) providing remuneration to authors; 2) ensuring the protection of investments made by producers and 3) providing the society broad access to cultural goods, are equally important goals or maybe the first two points are the means to realize the true purpose of copyright, as indicated in the third point.

The result of the use of the single term *rightholder* is that we think of a uniform legal construction through which we want to protect his interests. *If authors or performers are to continue their creative and artistic work, they have to receive an appropriate reward for the use of their work, as must producers in order to be able to finance this work (recital 10).* These two independent groups of actors that have different and sometimes divergent interests are to be protected by the same legal instrument which are *the exclusive rights*. It is obvious that provide for the authors *the right to remuneration for the exploitation of their works* is not the same as granting *the exclusive rights*.

Lyman Ray Patterson warned against the confusion of the interest of authors with the interests of the entities that manage or acquire copyrights.

"The source of the monopoly problem was not the author, but the publisher. The control of a given work, whether by the publisher or the author, of course, is a monopoly of that work. The difference in the danger, however, is in the source of control and, thus, in the number of works each may control. The publisher's source is contract with the author; the author's control results from the fact of his creation. It is one thing for a publisher to have a monopoly of the works he acquires from a number of authors and another for an author to have a monopoly of the work he creates"[11].

From the point of view of the *Authors*, the *right to remuneration*, can be regarded as a legal instrument sufficiently protect their interests[12]. From the point of view of *Copyright*

[11] L.R. Patterson, *Copyright in Historic Perspective*, Vanderbilt University 1968, p. 217.
[12] For the purposes of this article I omit discussion on whether *the right to remuneration* is generally a condition *sine qua non* for the emergence of creativity. It seems, however, that the right to remuneration - for authors - is equitable solution and not a necessary condition.

Management Entities such a right may be considered as insufficient to protect their independent interests. In this case, the position of the *Other Citizens* is closer to the position of *Authors* - because for the citizens of *the right to remuneration* is a legal instrument that is less restrictive than an *exclusive right*. But do we have to worry about the interest of the producers? It seems that *exclusive rights* help in the activities undertaken by the producers but they are not condition *sine qua non* of this activity. What is more, as pointed out by Carliss Y. Baldwin and Eric von Hippel the "producers' model" is just one of the model by which it is possible the emergence of creative work[13] For the existence and development of other models, not only *the exclusive rights* do not constitute a precondition but rather constitute an obstacle. This is particularly evident on the example of creativity emerging in the Internet, for example peer production and sharing[14].

4.3. Intangible goods should be treated as tangible goods that is, they should be (in each case) protected by exclusive rights?

The history of copyright law is associated with the history of the invention of the printing press. The possibility of mass copying of texts not only threatened the interests of the political and ecclesiastical authorities, but also exposed the interests of the newly formed professions which were printers and booksellers. Taking into account only the interests of these groups it has been assumed that the right holders shall have be entitled with *the exclusive right to copy*. This assumption was founded in the time of printing privileges and then was adapted to the needs of the new mechanism rhetorically called authors' rights (French *d'auteur*, German *Urheberrecht*) or copyright. The same assumption was adopted in the WIPO Copyright Treaty (1996) and in InfoSoc Directive.

Constructing copyright as exclusive rights is based on the wrong assumption. The exclusive rights are suitable for adjusting the rules for the use of the *things* (material objects); in contrast to the *works* (abstract/immaterial objects). From an economic perspective, tangible and intangible goods do not function in the same way. In simple terms we can say that tangible meet the definition of so-called *private good* and intangible can be defined in the language of economics as *public good.* Economists define a *private good* as being *rival* and *excludable*, whereas *public good* are *non-rival* and *non-excludable*. Good is *excludable* if it is possible to

[13] C.Y. Baldwin, E. Hippell, *Modeling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation*, "Harward Buisness School Working Paper", http://ssrn.com/abstract=1502864 or http://dx.doi.org/10.2139/ssrn.1502864 (access 18.04.2013).
[14] Y. Benkler, *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale 2006, http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf (access 17.02.2014), p. 59.

prevent people from having access to it. It is not only about the physical possibility of exclusion. We can say in the case of goods that are *non-excludable* if the costs of excluding nonpaying beneficiaries who consume the good are so high that no private profit-maximizing firm is willing to supply the good[15]. A *rival* good is a good whose consumption by one consumer prevents simultaneous consumption by other consumers. For instance, only one person can sit in a chair at the same time. The same goes for food: if I eat the sandwich, you cannot eat it. A *non-rival* good can be consumed (or used) by one individual without detracting, in the slightest, from the consumption opportunities still available to others from the same unit[16]. A good example of this are *works.* If I watch the picture or read a book that does not deprive others from being able to watch or read the same picture or book. That's why, because of the *rival* nature of things, tangible goods may be stolen, whereas intangible goods can be copied. Additional persons can use the copy, which quality is just as good as the original, despite the fact that the marginal cost of producing copies are close to zero. This is a feature of such goods which should be utilized. *Exclusive rights* prevent the public from using this feature fully.

The creation of artificial scarcity in the case of intangible assets aims to fit them - by force - to the rules which govern the material things. Economy of tangible goods is based on different principles than the economy of intangibles. Tangible property and copyright solve different problems. The consequences resulting from the exclusive ownership of tangible things are different from the effects of the copyright monopoly. Copyright monopoly was created in order to solve one problem - the incentive to invest. However, trying to solve one (hypothetical) problem copyright creates other such as: monopoly prices, transaction costs, blocking the development of new works, threat to freedom of speech and the right to privacy etc.

In the past, due to the available technology, *works* may have been treated as *rival* good. In practice, it was impossible to read a book (immaterial object) without having access to its physical copy (material object). Digital technology made it possible to separate, once and for all, intangible *works* from their physical copies. In the case of *non-rival* goods from the economic perspective more efficient (static) is to provide broad access to such goods[17]. The Internet has enabled us to distribute and copy *works* at near-zero marginal cost. If we agree that the Internet has created new opportunities for human communication and creativity, it must be

[15] R. Cooter, T. Ulen, *Introduction to Law and Economics*, 2007, http://works.bepress.com/robert_cooter/56, p. 45.
[16] R. Cornes, T. Sandler, *The theory of externalities, public goods and club goods*, Cambridge 2003, p. 8.
[17] Free distribution, however, could cause problems for creating incentives for the production of innovation, and that is the dynamic issue. At the same time the creation of exclusive rights gives rise to the so-called *dynamic costs* see further: J. E. Stiglitz, *Economic foundations of intellectual property law*, "Duke Law Journal" 2008/57, p. 1706.

emphasized that the current copyright law – based on *exclusive right* - is trying to reduce all of these benefits.

4.4. Private use causes the prejudice to rightholders and digital private copying has a greater negative economic impact on the rightholders than analogue private copying

Since the beginning of industries whose business models are based on copyright public opinion constantly hears about the phenomenon called piracy. Organisations of these industries present us with a frightening calculation of the losses that are caused by pirates. Losses are presented at three levels: **(1)** direct losses to the film and music industry: MPAA: $ 6 billion losses for the film industry in the US (2005) and RIAA: $ 5 billion losses for the US recording industry (2005). According to the authors of these calculations, these losses are also translated into (2) losses to entire national economies (among others): $ 6 billion losses for the film industry is a $ 20.5 billion losses for the US economy, and the $ 5 billion losses for the record industry is a $ 12.5 billion losses for the US economy. Of course, this level of losses - in their opinion - will inevitably be reflected in **(3)** loss of jobs (among others): 373 000 lost jobs in the United States in the 2005 and the 611 000 - 1 217 000 lost jobs in the EU between 2008-2015[18].

These data, however, for a long time raise some doubts. Global box office for all films released in each country around the world reached $36.4 billion in 2014, up 1% over 2013's total. International box office in U.S. dollars is up 24% over five years ago, global box office is up 15% in the same time period[19]. If piracy is so big, how is it possible that the revenues of copyright industries grow? It is clear that uploading the film on the Internet before its premiere causes enormous losses to the producer! That's why The Dark Knight (2008), which was available on the Internet before its premiere was one of the most downloaded film of this period and at the same time bringing revenues of $ 1 billion. It is clear that file sharing causes a drop in interest among producers of films and music to invest! That is why the number of music albums that were released in the year 2000 was 35 516, while in 2007 only 79 695 and the number of films produced in 2003 decreased from 3 807 to 4 989 in 2007. It is obvious that, since so much music is available for free ... This causes the total consumer spending associated with music grew from $1.3 billion in 1998 to $4.2 billion in 2008[20]. It is clear that the shutdown of the largest pirate site (Megaupload) will cause the ... that box office revenues of a majority

[18] Based on J. Karaganis, *Rethinking piracy* [in] *Media piracy in emerging economies*, J. Karaganis (ed.), Social Science Research Council 2011, http://www.scribd.com/doc/50196972/MPEE-1-0-1 (access 01.05.2012), p. 12.
[19] Theatrical market statistics 2014, MPAA, http://www.mpaa.org/research-and-reports/ (access 14.03.2015), p.
[20] Data based on Karaganis J., *Rethinking piracy…*, p. 41-45.

of movies did not increase. While for a midrange of movies the effect of the shutdown is even negative, and only large blockbusters could benefit from the absence of Megaupload[21].

As pointed out by Joe Karaganis there are at least two reasons why the data presented by these organizations are misleading:

- the *substitution effects* —that is, the likelihood that a pirated copy substitutes for a legal sale—and the importance of the price/income effects in that determination; and
- the *countervailing benefits* of piracy to both industry and consumers in any model of total economic impact and, consequently, the importance of treating piracy as part of the economy rather than simply as a drain on it.

Substitution effects

In short, we can say that for long time industry research was based on assumption of one-to-one equivalence between pirated copies and lost sales. As a result, it was considered that one pirate copy (digital or analog) is responsible for (*substitute*) the lost sales of one legal copy. Such an assumption is obviously unrealistic. Independent researchers are trying to determine the answer to the question to what extent the informal channels of communication (including but not limited to pirated copies) replace the formal channels. Results of these studies can be divided into two groups. The first group includes such research, the results of which indicate the existence of a substitution effect. But this is not the result of one-to-one, but much (much) lower. Rafael Rob and Joel Waldofogel study the survey responses of a convenience sample of U.S. college students in 2003. They found that the each album download reduces CD purchases by between 0,1 and 0,2[22]. In 2006 Alejandro Zentner in his paper estimate that downloads may explain a 30% reduction in the probability of buying music[23]. Using a new survey of University of Pennsylvania undergraduates, Joel Waldofogel in 2010 ask how music file sharing and sales displacement operate in the iTunes era, when the alternative to file sharing is purchasing individual songs, rather than entire albums. In this sample, as in most other studies of the effect of file sharing, downloaded music reduces purchased music, by between 0.15 and 0.28 per downloaded song[24]. The second group includes such research, the results of which indicate lack

[21] Ch. Peukert, J. Claussen, T. Kretschmer, *Piracy and Movie Revenues: Evidence from Megaupload: A Tale of the Long Tail?*, http://ssrn.com/abstract=2176246 or http://dx.doi.org/10.2139/ssrn.2176246 (access 12.09.2014), p. 19.

[22] R. Rob, J. Waldfogel, *Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College, Student*s, National bureau of economic research 2004, Working Paper 10874 http://www.nber.org/papers/w10874 (access 14.03.2015), p. 28.

[23] A. Zentner, *Measuring the Effect of File Sharing on Music Purchases*, "J. Law and Econ." 49 (April): 63–90. 2006, p. 87.

[24] J. Waldfogel, *Music File Sharing and Sales Displacement in the iTunes Era*, "Information Economics and Policy" 2010/22, p. 15.

of substitution effect. For example, David Bounie, Marc Bourreau and Patrick Waelbroeck studied which, if any, segments of the movie business have suffered from digital piracy. They use a sample of 620 university members including undergraduate students, graduate students. "For movie theaters, we do not find any significant negative effect of the intensity digital piracy. As a matter of fact most coefficients associated with piracy have a positive sign"[25]. Felix Oberholzer-Gee and Koleman Strumpf matched an extensive sample of downloads to U.S. sales data for a large number of albums. "Using detailed records of transfers of digital music files, we find that file sharing has had no statistically significant effect on purchases of the average album in our sample"[26]. Currently, it can be stated that while the majority of empirical studies indicates the possibility of the existence of the substitution effect, none of them indicate the possibility of accepting the assumptions of one-to-one[27].

On this background interesting results can be found in the report titled "Ups and downs. Economic and cultural effects of file sharing on music, film and games". It states that: "Generally, file sharing and buying go hand in hand. Consumers who download tend to be aficionados of music, films or games, which therefore play an important role in their daily lives. Among music and film downloaders, the percentage of buyers is just as high as among non-downloaders; among game sharers, the percentage of buyers is even higher than among people who do not download games. In addition, music downloaders have been found to go to concerts more and to buy more merchandise. Game sharers buy more games a year than gamers who do not download and film sharers tend to buy more DVDs on average than do non- file sharers" [28].

Countervailing benefits

Speaking of downloading, we can not only focus on the loss of industry. We should understand the importance of *countervailing benefits* to both industry and consumers, that is treating unauthorized copying as a part of the economy rather than simply drain on it. That is

[25] D. Bounie, P. Waelbroeck, M. Bourreau, *Piracy and the Demand for Films: Analysis of Piracy Behavior in French Universities*, "Review of Economic Research on Copyright Issues" 2006/2, http://ssrn.com/abstract=1144313, (access 13.10.2014), p. 23.
[26] F. Oberholzer-Gee, K. Strumpf, *The Effect of File Sharing on Record Sales: An Empirical Analysis*, "Journal of Political Economy" 2007/1, p. 38.
[27] See further: M.D. Smith, R. Telang, *Assessing the academic literature regarding the impact of media piracy on sales*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2132153 (access 12.12.2014), S. Dejean, *What can we learn from empirical studies about piracy?*, "CESifo Economic Studies, Oxford University Press (OUP): Policy E - Oxford Open Option D" 2009/2, https://hal.inria.fr/file/index/docid/963851/filename/1draft.pdf (access 12.12.2014).
[28] A. Huygen, N. Helberger, J. Poort, P. Rutten, N. van Eijk, *Ups and Downs; Economic and Cultural Effects of File Sharing on Music, Film and Games* (February 18, 2009) "TNO Information and Communication Technology Series", http://ssrn.com/abstract=1350451 or http://dx.doi.org/10.2139/ssrn.1350451 (access 10.09.2014), p. 4.

why we should look at downloading and file sharing as a transfer of income in a whole economy – not as a loss on specific industrial sector. Money saved by consumers on traditional way of acquiring cultural products can be spent on others (new one). "[C]onsumer surplus from piracy might be more productive, socially valuable, and/or job creating than additional investment in the software and media sectors"[29]. For example, as demonstrated by research conducted by Joel Waldofogel[30] in 2010, file sharing raises per capita consumer surplus by $11.91, of which $1.00 is revenue lost by sellers and $10.91 is reduced deadweight loss[31]. Estimates made in the report entitled "Ups and downs. Economic and cultural effects of file sharing on music, film and games" showed that the consumer surplus created by music sharing in the Netherlands would then amount to an estimated minimum of €200 million per year[32]. When this amount is subtracted from the potential losses of producers[33], turn the economy as a whole comes out on the plus side, which is €100 million per year. What's more, as noted by Sylvain Dejean, even if we admit that piracy is globally detrimental for cultural industries, strong evidences show that it could be locally beneficial for unknown and new artist. "As a result piracy forces the business model of cultural industry to evolve towards less concentration of sales, a shift in the distribution of revenue between the actors of the industry and the recognition of the competition with new medias appeared with the rising of the internet"[34].

[29] J. Karaganis, *Rethinking piracy…*, p. 16.
[30] J. Waldfogel, *Music File Sharing and Sales Displacement in the iTunes Era*, "Information Economics and Policy" 2010/22, p. 15.
[31] In economics, a deadweight loss is a loss of economic efficiency that can occur when equilibrium for a good or service is not achievable. Causes of deadweight loss may be the imposition of monopoly prices for the created artificial scarcity of goods by copyright. See further K. Gliściński, *Rola modelu ochrony dóbr niematerialnych w ramach Społecznego Systemu Wspierania Innowacji — zarys analizy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej" 2013/3.
[32] A. Huygen, N. Helberger, J. Poort, P. Rutten, N. van Eijk, *Ups and Downs…*, p. 107.
[33] This is equivalent to a substitution ratio of at most 5-7%, or one track less sold for every 15 to 20. Huygen A., Helberger N., Poort J., Rutten P., Eijk N. van, Ups and Downs; Economic and Cultural Effects of File Sharing on Music, Film and Games (February 18, 2009) "TNO Information and Communication Technology Series", http://ssrn.com/abstract=1350451 or http://dx.doi.org/10.2139/ssrn.1350451 (access 10.09.2014), p. 102.
[34] S. Dejean, *What can we learn from empirical studies about piracy?* "CESifo Economic Studies" 2009/2, p. 20.

5. Conclusions

The purpose of the article was to show why the assumptions on which ware based the judgment C 435/12 and Directive are wrong. Correction of these assumptions, which will take into account the current knowledge on the functioning of intangibles, allows for the correct interpretation of the law of the European Union. That why in my opinion we should not focuses only on rightsholder hypotheetical losses as Court did in Case C-435/12. We should better understand the functioning of intangible goods. We should see copyright in broader perspectives (social roles of copyright*). Efforts to quantify the economic value of intellectual property should reflect the economic value attributable to activities enabled by limitations and exceptions to intellectual property rights, openness policies and practices, and the public domain*[35]. Since copyright is a means to achieve an important social purpose, and not a goal in itself we should replace (in some cases) *exclusive rights*, the *right to adequate remuneration*.

From a legal point of view, interpreting the provisions of the Directive, the court should take into account greed statement to Article 10 of WIPO Copyright Treaty (1996) which states that these provisions should be understood to permit Contracting Parties to devise new exceptions and limitations that are appropriate in the digital network environment. In view of *countervailing benefits* and the benefits of *non-rival* nature of the intangible goods *recital 38* in the preamble to Directive, which indicates the need for a separate treatment digital and analogue private copying, should be interpreted as allowing the full realization of these benefits. In the same direction, due to low levels of *substitution,* it should be interpreted *recital 35* which provides that in certain situations where the prejudice to the rightholder would be minimal, no obligation for payment may arise. Considering also that the primary purpose of copyright is to providing the society broad access to cultural goods without undermining values such as freedom of speech and the right to privacy and taking into account the risks of monopoly it should be concluded that:

EU law, in particular Article 5(2)(b) of Directive 2001/29/EC, read in conjunction with paragraph 5 of that article, lege non distinguente includes both cases, that is situation in which the source from which a reproduction for private use is made is lawful and in which that source is unlawful.

[35] Washington Declaration on Intellectual Property and the Public Interest, http://infojustice.org/washington-declaration-html (access 19.02.2014).

Chapter 3

WHAT IS DONE CANNOT BE UNDONE. THE CHANGING FACE OF INTELLECTUAL PROPERTY LAW IN THE MEDIA SOCIETY

Karolina Sztobryn

Ph.D, University of Lodz, Faculty of Law and Administration, Department of European Economic Law, Kopcinskiego 8-12, 90-232 Lodz, Poland, ksztobryn@wpia.uni.lodz.pl

Keywords: *intellectual property rights, copyright, protection of computer programs, exhaustion of rights*

Abstract: *There is a strong relationship between the media and intellectual property. On the one hand, intellectual property goods are created because they are transmitted through the media, on the other hand media can only work by creating goods of intellectual property. The development of media society set before intellectual property law many challenges. Both law practitioners and academics ask whether the law follows the media and their spectacular development, and whether the law meets expectations of media society. The answers to these questions are negative, but fortunately law tries not to be further than a step behind the progress, not only by creating new legal frameworks that meet the needs, but also, and perhaps above all, thanks to the progressive interpretation of traditional legal rules.*

1. The die is cast

The ubiquity of communication media is now so obvious that we often do not perceive in how many situations of everyday life we use them. Radio, television and the Internet accompany us at every step, and through these media we face with intellectual property. There is a strong relationship between the media environment and intellectual property. On the one hand, goods protected by intellectual property law are communicated to the public through the media. On the other hand, media activities largely depend on intangible property, what can be manifested in two ways. Firstly, the technical ability to perform media activities is based on inventions often protected by patent law, which allow the transmission of information.

Secondly, media activities are based on the presentation of intangible goods, such as cinematographic and music works. Therefore, it can be concluded that the media are the aggregates of intellectual property, i.e. works, trademarks, and patents. Functioning and also the use of media would not be possible without intangible property. Copyright protection covers a ringtone, announcing that someone is trying to reach you, a photo you send as MMS or through Facebook, a song, you listen on the radio, and a movie that we watch on TV or YouTube.

The development of the media environment poses before intellectual property rights many challenges relating in particular to the creation of new intangible goods, whose protection by the traditional intellectual property rules was doubtful; and to the need of applying existing regulations of intellectual property law to the new forms of media communication, including the Internet. Both practitioners and legal academics across Europe often consider the question whether the law follows the development of media and responds to the media society needs. The answer to these questions is unfortunately negative, but fortunately the law tries not to be further than a step behind the progress, not only by adapting existing regulations to new needs or creating completely new regulations, but also, and perhaps above all, thanks to the progressive interpretation of the traditional principles of intellectual property rights made by the courts, mainly the Court of Justice.

2. Half a loaf is better than none

The creation and the development of the media environment are also associated with the development of new products that are part of this environment. These products may be a result of intellectual human activity, and therefore enjoy protection of intellectual property rights. However, not all effects of such intellectual efforts, due to their specificity, can be protected by traditional rules of intellectual property law. Therefore, with regard to certain goods, for example databases[1], the EU legislator decided to establish a system of protection based on the new rules, created specifically for this type of products. But not all new media products enjoy a *sui generis* protection. In many cases, the protection of new goods is based on the traditional intellectual property rules, like in relation to computer programs. The inclusion of computer programs to already existing rules caused concerns that the current protection of these goods is inadequate to their real needs.

[1] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ L 77, 27.3.1996, p. 20–28.

The primary protection model of computer programs is based on the copyright law, which is the result of adaptation of the Directive 2009/24/EC on the legal protection of computer programs[2]. A computer program is a creation of the human mind, which can be expressed in a variety of ways, i.e. source and object codes. However, it is not designed for esthetical purposes like all works protected by copyright law, but for utility reasons, and is situated on the borderline of text, function and information[3]. The Directive 2009/24/EC protects only the program codes, thus the scope of protection of the computer program is not adequate to its needs, as it does not cover utility and functional elements of the program. Whilst, the software program is the most important for its usefulness and functionality, the copyright law traditionally emphasizes the individual nature of the program. In my opinion, attempts to make a broad interpretation of the copyright provisions for the purpose of computer program protection are not appropriate, as they may lead to legal uncertainty. Extending the copyright protection to intangible goods of utilitarian nature shows, however, that the original goal of copyright law relating to the protection of purely intellectual works, such as literary and artistic works, has evolved to include the protection of functional immaterial goods that can be used in the industry[4].

Functional elements of computer programs implemented in the invention may still be protected by a patent, despite the exclusion of computer programs as such from patentability in accordance with Article 52 (2) (c) of the Convention on the Grant of European Patents (EPC)[5]. The patent system protects against achieving the same effects as included in the protected program, and because of the functional nature of computer programs, may seem more appropriate for the protection of these goods than the copyright law. However, the European Patent Office interprets the conditions for patentability of computer programs (technical nature, novelty, inventive step and industrial application) in the traditional way, therefore patent protection for many inventions containing computer programs is denied.

Although the above indicated protection models of computer programs have their supporters and opponents[6], it is generally agreed that they are both not perfect. Copyright

[2] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, OJ L 111, 5.5.2009, p. 16–22.
[3] H.C. Anawalt, *International Intellectual Property, Progress, and the Rule of Law*, Santa Clara Computer and High Technology Law Journal 2003/19, p. 389; compare: J. Ożegalska-Trybalska, *Ochrona programów komputerowych i wynalazków implementowanych za pomocą komputera* [in:] *Komputer – Człowiek – Prawo*, W. Lubaszewski (ed.), Kraków 2007, p. 112.
[4] Compare: T. Cook, *EU Intellectual Property Law*, Oxford 2010, p. 68.
[5] Convention on the Grant of European Patents, OJ EPO 2001, special edition no. 4, p. 55.
[6] See: K. Sztobryn, *Ochrona programów komputerowych w prawie własności intelektualnej Unii Europejskiej*, Warszawa 2015, p.

protection covers creative expressions and therefore it does not correspond to the nature of computer programs, which are indeed expressed in the form of text, but only as a sequence of instructions for a specified task. Furthermore, this regime does not seem adequate to fulfil the economic purposes of the protection[7]. Traditional protection under patent system might, in turn, jeopardize the creation of new competitive and compatible programs, while the creation of programs requires a joint and sequential development and re-use of other developers' works[8]. Also in terms of the duration of protection, the traditional intellectual property rules do not correspond to the needs of computer programs. Copyright law affords a 70-year protection while the term of the patent is generally 20 years. Software utility lasts for three to ten years, and an average five years[9].

It appears that the current legislation fails to adequately protect one of the most important products used in the media society, namely computer programs. The Court of Justice tries to alleviate some of these deficiencies by interpreting the Directive 2009/24/EC in a manner corresponding to the major changes in the distribution of intangible goods, what will be mentioned later in this paper.

3. Store is (no) sore

Adapting the law to the needs of the media environment occurs also through enacting new legislation and changing the law already in force. An example of such a new act is the Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society[10]. The Directive 2001/29/EC is the result of efforts taken in the 1990s in the EU towards harmonizing the laws of the Member States relating to the protection of

[7] D.G. Luettgen, *Functional Usefulness vs. Communicative Usefulness: Thin Copyright Protection for the Nonliteral Elements of Computer Programs*, "Texas Intellectual Property Law Journal" 1996/4, p. 273; C.M. Guillou, *The Reverse Engineering of Computer Software in Europe and the United States: A Comparative Approach*, "Columbia – VLA Journal of Law & the Arts" 1998/22, p. 555; G.R. Ignatin, *Let the Hackers Hack: Allowing the Reverse Engineering of Copyrighted Computer Programs to Achieve Compatibility*, "University of Pennsylvania Law Review" 1992/5, p. 2021; L. Egitto, *Certifying Uncertainty: Assessing the Proposed Directive on the Patentability of Computer Implemented Inventions*, "The Journal of Information, Law and Technology" 2004/3 http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/egitto/ (available: 12.1.2015); J.C. Philips, *Sui Generis Intellectual Property Protection for Computer Software*, "The George Washington Law Review" 1992/60, p. 1007; A. Esteve, *Patent Protection of Computer-Implemented Inventions Vis-À-Vis Open Source Software*, "The Journal of World Intellectual Property" 2006/3, p. 288.

[8] H.W.A.M. Hanneman, *The Patentability of Computer Software*, Boston 1985, p. 9; S. Perchaud, *Software Patents and Innovation*, "Journal of Information, Law & Technology" 2003/1, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/perchaud/ (available: 12.01.2015 r.).

[9] M. Campbell-Kelly, P. Valduriez, *A Technical Critique of Fifty Software Patents*, "Marquette Intellectual Property Law Review" 2005/2, p. 273–274; E. Gratton, *Should Patent Protection Be Considered for Computer Software-Related Innovations?*, "Computer Law Review & Technology Journal" 2003/7, p. 231.

[10] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10.

works[11]. How strong was the need to introduce an act answering to the increasing digitization of creative content, is evidenced by the fact that since the beginning of work on the Directive 2001/29/EC many issues have not been widely discussed and debated, while they were uncontroversial[12]. In practice, however, provisions of the Directive often raised doubts of the national courts and had to be interpreted by the Court of Justice.

The Court of Justice ruled, inter alia, that the signal distribution via television sets installed in hotel rooms by a provider of accommodation services constitutes communication to the public within the meaning of Article 3 (1) of the Directive 2001/29/EC, regardless of the technique used to transmit that signal[13], and that a Member State may grant public libraries the right to digitize works which are contained in their collections, if such act of reproduction is necessary for the purpose of making those works available to users, by means of dedicated terminals within those establishments[14].

The number of entirely new legislative acts in the field of intellectual property rights is not particularly spectacular, and that would be expected considering the progress observed with respect to communication media. Consequently, it raises many questions: maybe this progress is not significant enough to require new legislations? Or maybe the respective needs are not noticed by the legislators? Or maybe the existing rules are so progressive (or general), that there is no need for a new regulatory approach?

I believe that each of these questions should be answered partly positive. Legal amendments are also not introduced due to the social opposition to reforms responding to technological development. The most significant example of such a resistance on a European scale was the protest against ACTA[15]. Recently, in Poland, part of the media society has opposed to the proposal[16] to adapt the law to technical progress in the form of changing Polish

[11] European Commission Green Paper of 27 July 1995 on Copyright and Related Rights in the Information Society [COM(95) 382 final; *Europe's Way to the Information Society: an Act on Plan* Communication from the Commission to the Council and the European Parliament and to the Economic and Social Committee and the Committee of Regions, COM(94) 347 final, Brussels, 19 July 1994].
[12] T. Cook, *EU Intellectual Property Law*, Oxford 2010, p. 93.
[13] Court of Justice: C-306/05, *Sociedad General de Autores y Editores de España (SGAE) v Rafael Hoteles SA*, 7.12.2006, ECLI:EU:C:2006:764; Court of Justice: C-162/10, Phonographic Performance (Ireland) Limited v Ireland and Attorney General, 15.3.2012, ECLI:EU:C:2012:141.
[14] Court of Justice: C-117/13, *Technische Universität Darmstadt v Eugen Ulmer KG*, 11.9.2014.
[15] Proposal for a Council decision on the conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, COM/2011/0380 final.
[16] Statement of the Minister of Culture and National Heritage of 8.10.2015 http://www.mkidn.gov.pl/pages/posts/oswiadczenie-mkidn-dotyczace-oplaty-reprograficznej-5034.php?searchresult=1&sstring=nośników (available: 18.2.2015)

regulation[17] containing a list of devices and media used for recording works[18], on which fees, called copyright levies, are imposed. The essence of these fees is to compensate developers the potential benefits that they could have lost due to so-called private copyright, which allows the society to make copies of works by means of technological devices for their own individual purpose. These fees are added to the sale price of reproduction devices in case they are used for copying works for private use. Consequently, they are borne by the final consumer and transferred by the producers of these devices to the collecting management organizations. In this article I am not able to point all the problems that are associated with copyright levies, and they are indeed numerous, as evidenced by the Court of Justice judgments[19] and increased list of reports prepared for the European Commission[20]. Here I will only try to demonstrate that currently the final version of each act relating to intellectual property is a result of strong influence of media society, as in case of plans to expand the list indicating the carriers and media on which copyright levies are imposed. In Poland this list currently includes, among others, such "old" media and devices as cassettes, CDs and cassette radios. The plan is to cover by this fees also reprographic equipment actually used by the society media for copying for private purposes, even if the coping function of these devices is only secondary to the primary function they serve. While in Poland this debate is gaining momentum, in Austria, for example, the Supreme Court held that tablets and personal computers should be subject to copyright levies. And here we face another legal problem, which relates to the differences between the lists of devices covered by the fees and the amount of these charges across the EU.

Diverse systems of copyright levies may constitute an obstacle to the functioning of the internal market, as the same goods may be subject to a fee in one Member State, for example in Finland, whereas in another, for instance in Poland, not. Undoubtedly, the most effective

[17] Regulation is one of the universally binding source of law in Poland, in addition to the Constitution, ratified international agreements, acts (pol. ustawa) and local acts. It is a normative act issued on the basis of specific authorization contained in acts, and for its implementation.

[18] Regulation of the Minister of Culture of 2 June 2003 On determining the categories of devices and media used for recording works and charges on these devices and media from their sale by manufacturers and importers Journal of Laws of 2003, No. 105, item 991 (Rozporządzenie Ministra Kultury z dnia 2 czerwca 2003 r. w sprawie określenia kategorii urządzeń i nośników służących do utrwalania utworów oraz opłat od tych urządzeń i nośników z tytułu ich sprzedaży przez producentów i importerów, Dz.U. 2003 nr 105 poz. 991).

[19] Court of Justice: C- 463/12, *Copydan Båndkopi v Nokia Danmark A/S*, 5.3.2015, not published; Court of Justice: C-467/08, *Padawan SL v Sociedad General de Autores y Editores de España (SGAE)*, ECLI: ECLI:EU:C:2010:620.

[20] A.Vitorino, *Recommendations resulting from the mediation on private copying and reprography levies*, Brussels, 31.1.2013, http://ec.europa.eu/internal_market/copyright/docs/levy_reform/130131_levies-vitorino-recommendations_en.pdf (available: 18.2.2015); M. Kretschmer, *Private Copying and Fair Compensation: An empirical study of copyright levies in Europe*, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/310183/ipresearch-faircomp-201110.pdf (available: 18.2.2015).

way to solve this problem would be a full harmonization of copyright levies system, which would include the rates as well as the list of devices and media subject to these fees. However, in fact, such harmonization could cause more detriment than benefit to the media society in the EU. It is worth noting that there are still some discrepancies in the use of media facilities by EU citizens in particular Member States. Also, awareness and purchasing power of consumers is different. Therefore, Member States should be allowed to draft their copyright levies systems individually in order to adapt them to the social needs and cultural traditions, as well as be able to intervene promptly when the changes are needed.

4. When two dogs fight for a bone, third does (not) run away with it

Also the courts are facing the challenges resulting from technological development in the field of intangible assets. In many cases courts' interpretation of intellectual property concepts, leads to their evolution.

In the case of trade marks, the courts were, until recently, mainly examining the similarity of trade marks for purposes of registration and infringement proceedings. Whereas today, the courts are often required to resolve seemingly fundamental problems namely, whether the use of the trade mark constitutes a violation of trade marks rights, and if so, who is responsible. This problem arises, for example, in the case of the sale of goods bearing the trademarks through the internet portals which enable the sale and purchase of goods, such as eBay or Allegro, and in the case of the so-called keyword advertising on search engines. Specific problems associated with the use of trademarks by third parties in both types of cases have been analysed by the Court of Justice. For the purposes of its analysis the Court extended the circle of potential violators by introducing the concept of primary and secondary infringement[21]. The former can be committed by entities, which actually use someone else's trade mark, so by the sellers or advertisers of goods. The latter concerns entities, which do not use the trade mark, but provide services enabling the sale of goods (Allegro or eBay) or presentation of advertisement (Google). Secondary liability of service providers occurs when the conditions indicated in Article 14 (1) of the Directive 2000/31/EC[22] do not apply and the operator of the online marketplace plays an

[21] Court of Justice: C-324/09, *L'Oréal SA and Others v eBay International AG and Others*, 12.6.2011, ECLI:EU:C:2011:474; Court of Justice: C-236/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, C-237/08, *Google France SARL v Viaticum SA and Luteciel SARL*, and C-238/08, *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others*, 23.3.2010, ECLI:EU:C:2010:159

[22] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1–16.

active role in the presentation of content on his networks, which allows him to obtain the knowledge about the stored data or to exercise control over them. If, for example, the operator supports the advertiser or the seller by optimizing the presentation of specific offers, he can be deemed responsible for the content of the stored data[23].

5. The exception does not prove the rule

Among all the forms of society media communications, the Internet poses the greatest challenge not only on the above-described trade mark rights grounds. The Internet not only provides access to a large amount of information placed on the network, but also enables copying, interfering in the content of works and forwarding them[24]. Therefore, the Internet is also a source of problems for the application of traditional copyright rules, which are often resolved by the courts through an evolutionary interpretation of the provisions of this law in order to apply them in the media environment. The concept of exhaustion of the right to distribute a computer program was the subject of such a progressive interpretation.

The principle of exhaustion of rights, which applies generally to all intellectual property rights, provides that with the first sale of copies of the work (including computer software), or of the goods bearing the trade mark, or other goods, in which intellectual property rights have been embodied, by the proprietor or with his consent, exhaust the distribution right of that copy or good bearing the trade mark[25]. Although this principle applies to all items in which intellectual property rights are embodied, the exhaustion of rights is generally limited to the goods in the material form and does not extend to the sale of digital copies via the Internet. It is different, however, in the case of exhaustion of the right to distribute a copy of a computer program. In the judgment *UsedSoft GmbH v. Oracle International Corp.* [26] the Court of Justice treated the exhaustion of the right to distribute computer software on tangible and on intangible media synonymously, because he considered that "the EU legislator equated both kinds of program distribution"[27].

---

[23] Court of Justice: C-324/09 L'Oréal SA and Others v eBay International AG and Others, par. 116; Court of Justice: C-236/08, *Google France SARL and Google Inc. v Louis Vuitton Malletier SA*, C-237/08, *Google France SARL v Viaticum SA and Luteciel SARL* and C-238/08, *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others*.

[24] A. Endeshaw, *Reconfiguring Intellectual Property for the Information Age: Towards Information Property?*, "The Journal of World Intellectual Property" 2004/3, p. 339.

[25] Article 4 (2) of the Directive 2001/29/EC; Article 4 (2) of the Directive 2009/24/EC; Article 7 of the Directive 2008/95.

[26] Court of Justice: C-128/11*, UsedSoft GmbH v Oracle International Corp*, 3.7.2012, ECLI:EU:C:2012:407.

[27] Court of Justice: C-128/11*, UsedSoft GmbH v Oracle International Corp*, par. 58.

Although the conclusion of the Court is essentially correct, it can be questioned whether at the time of creating the original version of the Directive 91/250/EEC, now codified as the Directive 2009/24/EC, but whose provisions in this regard have not changed, i.e. in the 1980s, the EU legislator could have thought that in the future, computer programs will be available to users online. However, both from the legal and economic point of view, distributing the program in a material or an immaterial form is associated with the same consequences. Online transmission of the program can be regarded as a functional equivalent of the transfer in the material form, and the fee, often called by the proprietor "a license fee", is equivalent to the remuneration for the transfer of ownership of a program copy.

The inclusion of online software distribution to the legal consequences of the principle of exhaustion of rights was a necessary step in the light of the changing marketing techniques. However, modern forms of distribution do not only apply to software, but also to other digital products. Therefore, it may be doubtful, why the Court of Justice acknowledges the consequences of exhaustion with regard to the works sold online on the basis of the Directive 2009/24/EC, and so far refuses to accept them in relation to other works, for which the principle of exhaustion has been established in Article 4 (2) of the Directive 2001/29/EC. Such diverse treatment of particular types of works results from the different content of provisions applicable to them. Recital 29 of the Directive 2001/29/EC clearly indicates that "the question of exhaustion does not arise in the case of services and on-line services in particular"[28]. Perhaps the Court of Justice shares the view that "on-line distribution is not in fact distribution at all, but rather an invitation to access databanks which hold those digital publications"[29].

6. Standing still is to move back

New face of intellectual property rights indicated in this article are the best proof that the technological changes in field of new media are also reflected in the changes of intellectual property law. Trends in creating the image of the intellectual property rights include:

- Greater harmonisation and even unification of laws of the EU Member States.

Although intellectual property rights are still notably national rights (based on EU directives), the example of trademarks and designs as well as an attempt to create a patent with unitary effect in the EU[30] proves the increased recognition of the need to protect intangible goods in

[28] Directive 2001/29/WE, recital 29.
[29] J. Cameron, *[Opinion] Approaches to the Problems of Multimedia,* "European Intellectual Property Review" 1996/3, p. 118.
[30] Regulation (EU) No 1257/2012 of the European Parliament and of the Council of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection, OJ L 361, 31.12.2012,

the whole EU. In view of the society needs, it is not possible to completely eliminate national intellectual property rights and to establish a comprehensive and uniform regime for the protection of intangible assets in the EU. Member States should still be free to adopt laws corresponding to the needs of their media society. Given the often-divergent interests of the Member States it is also not possible to standardize all aspects of intellectual property rights. Therefore, the approximation of the laws of the Member States seems to be an effective and for now appropriate form of the creation of intellectual property rights in the EU.

- Refraining from creating new *sui generis* protection systems for emerging new intangible goods. It is difficult to create completely new models of protection for all emerging creations of the human mind[31]. However, this approach results in a change of the traditional character of copyright and industrial property. Consequently, copyright has become relevant to some utilitarian works, while industrial property rights may also apply to inventions, which are hardly technical[32]. Refraining from creating new models of protection for emerging new intangible goods might also leads to accumulation of rights to intangible assets on the bases of copyright and industrial property law. Therefore, it should be considered whether the rule currently in force "take as much as you can" should not be replaced by the principle "only one for everyone"[33].

- Significant role of the courts, in particular the Court of Justice, in the interpretation of the intellectual property rights concepts. The courts often see the need of progressive interpretation of the provisions corresponding to the technological reality. Where the existing legislation does not correspond to the technological development, this trend should be continued.

- Growing importance of the attitude of the media society. On the one hand, the growing awareness of the need to protect the intangible assets, on the other hand, a more demanding attitude of intangible goods users towards the proprietors, manifesting that information, also included in the protected goods, should be free and publicly available, causes the need to balance the protection of an individual and collective interests in the proposed

p. 1–8; Council Regulation (EU) No 1260/2012 of 17 December 2012 implementing enhanced cooperation in the area of the creation of unitary patent protection with regard to the applicable translation arrangements, OJ L 361, 31.12.2012, p. 89–92; Agreement on a Unified Patent Court, OJ C 175, 20.6.2013, p. 1–40.

[31] R.M. Ballardini, *Scope of IP Protection for the Functional Elements of Software* [in:] *In Search of New IP Regimes*, N. Bruun (ed.), Helsinki 2010, p. 49; M. Campbell-Kelly, P. Valduriez, *A Technical Critique…*, p. 280.

[32] A. Kopff, *Wpływ postępu technicznego na prawa autorskie*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace z Prawa Własności Intelektualnej" 1988/48, p. 61.

[33] D. Vaver, *Invention in Patent Law: A Review and a Modest Proposal*, "International Journal of Law and Information Technology" 2003/11; D. Vaver (ed.), *Intellectual Property Rights Critical Concepts in Law*, Oxford 2006, p. 77.

regulations. Otherwise, all legislative initiatives, even those serving a notable purpose, like protection of intellectual progress and innovation, may fail, as exemplified by the already mentioned ACTA.

Despite the changing image of the intellectual property rights over the last few years, it is clear that this area of law is just evolving, while technological changes can be described as a revolution. That is why the law will always be right behind the progress, and the task of lawyers should be to identify emerging legal issues and anticipate the need for future changes in intellectual property law. These problems and needs may require an adjustment of the law to new emerging intangible property goods and to a method of their protection. Currently, it is difficult to predict the trends in the interpretation of the intellectual property rights, but surely the development of law should take place in a sustainable manner just like technological progress. In both cases there is no way back, but it is difficult to indicate one single approach for the future.

Chapter 4

NEW METHODS OF PROCESSING PERSONAL DATA VS. PROFESSIONAL SECRECY OF LAWYERS. DIFFICULT RELATION? DATA PROTECTION PERSPECTIVE.

Katarzyna Witkowska

Ph.D. Student, University of Lodz, Faculty of Law and Administration; lawyer at Lubasz i Wspolnicy Law Office in Lodz, ul. Zwirki 17, 90-539 Lodz, Poland, katarzyna.witkowska@lubasziwspolnicy.pl;

Keywords: *Data protection, professional secrecy, confidentiality, new technologies, cloud computing*

Abstract*: Lawyers unlike many other professions are obliged to secure confidentiality and secrecy of all they get to know when providing their services. It means that they should act with greater care every time they decide to make use of a service, especially Internet-based one. Taking about lawyers in media society would be incomplete without paying attention to the rules of undertaking certain actions by lawyers themselves being a part of such society. Polish perspective and level of awareness of Polish lawyers in that field should also be taken into account in the discussion of new reality since the general idea of lawyers and media society concerns in fact lawyers providing legal aid in every country.*

1. Introduction

Lawyers unlike many other professions are obliged to secure confidentiality and secrecy of all they get to know when providing their services. It means that they should act with greater care every time they decide to make use of a service, especially Internet-based one. Taking about lawyers in media society (and that was the subject of the conference) would be incomplete without paying attention to the rules of undertaking certain actions by the lawyers themselves being a part of such society.

Scope of problems of media society with which lawyers have to deal in their day-to-day practice is very big. Use and misuse of technology, networks and criminal evidence, identify

theft, all the questions of e-commerce – these are just a few examples of how technology influences the fields of the legal practice. It is obvious that lawyers have to cope with them when providing their services. The other aspect of the problem is how lawyers deal with problems and challenges of new technologies when they are using it being at the same time obliged to keep full secrecy of all the information collected while providing a service.

The aim of this paper is to pay attention to the significant problem of new methods of processing personal data and data in general by lawyers (by the example of solicitors and barristers) obliged to provide confidentiality and secrecy when exercising their legal professions. It presents the abovementioned problem from the Polish perspective.

2. New technologies in legal practice

Undoubtedly, providing legal service nowadays requires a use of the new technologies. Digital environment in which also lawyers nowadays provide their services determines "how people communicate, consume […], how business organize themselves to make profits […], how engineers design and develop new technologies[1]. Rapidly changing world of technologies requires its subjects to invent new rules of conduct to guarantee that traditional values would still be effectively protected. "We have moved from a paper and text environment to one of electronic records and communications and the proper governance of maintaining confidentiality in electronic records and communications is hugely different to what is necessary in the text and paper environment"[2] Lawyers play very important role in this changing reality as it is their task to apply the law to this changing world. On the other hand, they are often users of the various technological solutions

One of the examples of commonly used technology is cloud computing used nowadays to facilitate storage of data and access to information from every device. Cloud computing as indicated by the Article 29 Data Protection Working Party can be understood as "a set of technologies and service models that focus on the Internet-based use and delivery of IT applications, processing capability, storage and memory space"[3]. As it is explained by the

[1] *The EDPS Strategy 2015-2019 Leading by example*, European data Protection Supervisor, accessible on the 17.03.2015 at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Strategy/15-02-26_Strategy_2015_2019_EN.pdf. p. 8

[2] *Information Security Guidelines for Law Firms,* Law Society of South Africa, guidelines accessible on the 9.03.2015 at http://www.lssa.org.za/upload/Information%20Security%20Guideline%202011.pdf

[3] *Opinion 05/2012 on Cloud Computing,* Article 29 Data Working Party accessible on 16.03.2015 at http://idpc.gov.mt/dbfile.aspx/WP196.pdf

Working Party, cloud computing can be a source of significant economic benefits and security benefits, but it can also create significant risks.

3. Polish perspective

Use of new methods of processing personal data in the legal practice should lead to the questions about securing confidentiality of data and legal rules and safeguards that should be applied when those new solutions are used.

First question that should be raised is the one about relation between data protection rules and professional secrecy of lawyers and application of the Act on Protection of Personal Data[4] to the legal activity. One of the most commonly repeated answers to the question about this relation is the one that professional secrecy eliminates the need for application of the data protection rules. This assumption is based on the article 3 paragraph 3 of Act on Legal Advisors[5] and article 6 paragraph 1 of Act on the Bar[6] that all introduce the rule of professional secrecy both for solicitors and barristers. Obligation to keep in secret everything that the lawyer gets to know during provision of the legal aid is treated as the circumstance exempting from the application of the obligations established in the Act on Protection of Personal Data on the grounds of its art. 5 that states "*should the provisions of any separate laws on the processing of personal data provide for more effective protection of the data that the provisions hereof, the provisions of those laws shall apply".* Abovementioned assumption concerning exemption from application of the Act on Protection of Personal Data is in fact completely wrong. Undoubtedly, professional secrecy constitutes particular legal regime, but it does not exclude and exhaust the data protection system. Specific characteristics of the provision of the art. 5 of Act on Protection of Personal Data lies in the fact that data protection act can give way to the other acts but only in narrow range – in the other aspects it should be applied.

Unfortunately, lawyers often limit protection of personal data to the professional secrecy, wrongly or mistakenly identifying the relationship between data protection and professional secrecy. Meanwhile, lawyers as many other data controllers process not only their clients' data but also data of their employees, business partners, potential clients, debtors and many others. These are types of data to which professional secrecy does not apply. If the art. 5 of Act on

[4] The Act of 29.08. 1997 on the Protection of Personal Data, Journal of Laws of 2014, item 1182 with amendments (pol. *Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych*, Dz. U. 2014.1182 z pozn. zm).
[5] The Act of 6.07.1982 on Legal Advisors, Journal of Laws of 2014, item 637 with amendments (pol. *Ustawa z dnia 26.05.1982 o radcach prawnych,* Dz. U. 2014.637 z pozn.zm)
[6] The Act of 26.05.1982 on Barristers, Journal of Laws of 2014, item 635with amendments (pol. *Ustawa z dnia 26.05.1982 prawo o adwokaturze,* Dz. U. 2014.635 z pozn. zm)

Protection of Personal Data is analyzed on the grounds of the protection of personal data in legal professions, it cannot be claimed that the classical relationship of *lex specialis derogat legi generali* occurs in this case. Acts concerning solicitors, barristers, legal counsels do not repeal application of the Act on Protection of Personal Data – they do it just in the scope arising from the professional secrecy. They do not contain regulations concerning, among others, procedures, data security, information obligations. Therefore, in this case, Act on Protection of Personal Data shall be applied.

The main point that should be understood is that on one hand legal activity is not limited only to the relations with clients, but also to many other types of relations and on the other hand, professional secrecy means only the obligation to keep the information in secret, but does not bring the answer to the question how to protect the information and by which means achieve security. Only if the abovementioned statement is correctly understood and the described relation is identified properly, security of the information and secrecy of data may be fully and effectively kept.

Secondly, presentation of the subject from the Polish perspective requires bringing attention to the problem of proper identification of the status of lawyer towards data collected from the client or in relation with the client's case and processed in order to provide a legal service. Lawyers who agree that data protection rules should be applied to their activity often have doubts if they are data controllers[7] or they just authorized to process data solely within the scope and for the purpose determined in a contract concluded in writing[8]. Proper qualification of this status is important as it implies scope of obligations arising from the Act on Protection of Personal Data incumbent on lawyers. Taking into account very few decisions of Polish Data Protection Authority – General Inspector for Data Protection that concern legal practice, the key to proper identification of the abovementioned status lays in the power of attorney that is granted to the lawyer by his client and that enables him to act on behalf of the client and in definitions proposed in the Directive 95/46/EC on the Protection of Individuals with Regards

[7] According to the art.7 point 4 of the Act on Protection of Personal Data*: controller - shall mean a body, an organizational unit, an establishment or a person referred to in Article 3, who decides on the purposes and means of the processing of personal data*. Article 3 indicate scope of the application of the Act on Protection of Personal Data by stipulating that: *The Act shall apply to state authorities, territorial self-government authorities, as well as to state and municipal organizational units. 2. The Act shall also apply to: 1) non-public bodies carrying out public tasks, 2) natural and legal persons and organizational units not being legal persons, if they are involved in the processing of personal data as a part of their business or professional activity or the implementation of statutory objectives - having the seat or residing in the territory of the Republic of Poland or in a third country, if they are involved in the processing of personal data by technical means located in the territory of the Republic of Poland.*

[8] In the meaning of the art. 31 of the Act on Protection of Personal Data

to the Processing of Personal Data and on the Free Movement of Such Data[9], implemented to the Act on Protection of Personal Data. In majority of cases lawyer working with a client should be treated as a subject authorized to process data pursuant to the contract not as a data controller. Legal activity should be though understood as a subsidiary one, in which lawyer (barrister, solicitor) processes data in order to achieve a goal indicated by his client. Lawyer in fact does not decide about purposes[10] of processing data, he just processes data pursuant to his client decision. The abovementioned qualification applies only to data processed in relation to provision of legal services (so to the data collected during management of the clients' cases and providing them legal aid), when a client – data controller grants a power of attorney to act on his behalf to the lawyer. In other cases, ex. as it comes to processing data of potential clients, clients (i.e. database of clients' personal data, not data processed in relation to the clients' cases), employees, contractors etc., lawyers are treated as data controllers.

Taking into consideration presented arguments, it should be underlined that Act on Protection of Personal Data applies to the services provided by lawyers and can be treated as a source of obligations for lawyers in case personal data is processed by them also with use of new technologies. According to the art. 36 paragraph 1 and 2 of the Act on Protection of Personal Data, the controller shall be obliged to implement technical and organizational measures to protect the personal data being processed, appropriate to the risks and category of data being protected, and in particular to protect data against their unauthorized disclosure, takeover by an unauthorized person, processing with the violation of the Act, any change, loss, damage or destruction. The controller shall also keep the documentation describing the way of data processing and measures referred to in paragraph 1. Lawyers are though obliged to design and implement personal data security policies and guidelines for application of informatics system. It is clear that maintaining data protection documentation can strengthen the data protection system only if applied in practice and obeyed at every step. It means that in legal practice every rule of conduct that concerns processing of data especially the data protected by the professional secrecy shall be carefully designed and deeply analyzed before applied in practice. Data protection should be treated by the lawyers as one of the crucial safeguards of providing the service in conformity with legal and deontological obligation of confidentiality and secrecy.

[9] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal L 281, 23/11/1995 P. 0031 - 0050*

[10] Nowadays it often happens that data controller, still having power of decision as the purpose of data processing in concerned, does not decide about means of processing data.

As it has been stated in title of the paper, relation between professional secrecy and processing of data in light of data protection rules seems to be difficult. This main section aimed to explain the reason for this relation being so difficult and to clarify the rules that should apply when legal requirements in the field of data protection and professional secrecy have to be combined. At the end of this section, couple of partial results of the research led by Center of Personal Data Protection and Management of Information at University of Lodz[11]. According to this unfinished research, about 90 % of lawyers claim that their team is obliged to keep the secret and 70 % claim that their system fulfills requirements imposed by the Act on Protection of Personal Information. In the meantime, 70 % of respondents have no data protection documentation implemented, 100 % of respondents have no data files registered and 100 % have not concluded the agreement authorizing to process data in which legal office or a lawyer would be subject processing data pursuant to the contract, 70 % them have not concluded such contracts as the data controllers. Those numbers, even if the research is still unfinished may show the general problem of lack of application of the data protection rules in the legal practice.

As the question of lawyers in media society is concerned, it should be underlined that there are no specific rules, guidelines or requirements established by specific chambers that would facilitate or enable use of technology by lawyers. In lack of such indications, one of the solutions can be to verify how this dilemma of technology on the doorstep of the legal office is solved on the international area by chambers from various countries from different data protection regimes.

4. International Perspective

4.1. CCBE Guidelines

Use of new technologies and new methods of processing data is for sure not irrelevant for the values that lawyers should or must protect. The topic itself is so important that it has become a leading matter of the guidelines elaborated and published by Council of Bars and Law Societies of Europe (hereinafter referred to as "CCBE")[12] for lawyers using cloud computing. The ideas included in the guidelines can serve as a very good example of the code of conduct when the choice of the service provider is done. The paper examines couple of crucial matters described by CCBE.

[11] Question forms for the research still accessible at http://wpia.uni.lodz.pl/struktura/centra-naukowe/centrum-ochrony-danych-osobowych/aktualnosci/item/568-ankiety

[12] *CCBE Guidelines on the use of cloud computing services by lawyers,* CCBE, 07.07.2012, Brussels

As it has been correctly indicated by CCBE use of cloud computing creates challenges, but also risks lawyers have to deal with. New technologies mean questions about privacy protection, professional obligation of confidentiality and other specific obligations incumbent on the lawyer[13]. CCBE underlines that "data protection rules and professional secrecy principles should be taken into account by lawyers as primary step when considering using cloud computing services"[14]. In Poland there are in fact no limitations in use of new technologies in codes of conduct and in specific laws designed for solicitors and barristers. In lack of such professional secrecy requirements, lawyers should apply data protection rules with even greater care.

The first issue that should be deeply examined in the process of choosing service provider is location of the service provider and its servers[15]. Risk of storing data outside European Union or European Economic Area in majority of cases can too high for lawyers as data stored outside EU data protection regime may be subject to the jurisdictions that do not require the same data protection standards as the EU and EEA countries do. Moreover, it may happen that data stored and located in the described way would be disclosed on the basis of national legal rules of the country of service provider, even without knowledge of the service user.

Moreover, CCBE highlights that legal office that undertakes decision about use of cloud computing service should necessarily take into consideration type of data that would be processed in the cloud[16]. Lawyers process mainly sensitive data, which requires higher level of protection. Sensitivity of data may imply application of more sophisticated technical, physical and organizational security measures. They should be applied by the lawyer processing data on the grounds of the agreement concluded with his client, but they are not limited only to this relation. Making use of cloud computing service does not exempt lawyer from assuring the same level of protection when processing od data is outsourced.

Furthermore, lawyer who decides to process data in the cloud should check if the possibility to engage sub-contractors is introduced to the agreement. CCBE indicates that such possibility should be excluded from the contract unless prior consent is obtained. The solution recommended by CCBE should be treated as the best one and particularly professionals bound by the obligation of confidentiality should pay attention to the provisions of contracts that

[13] *CCBE Guidelines on…,* p. 4.
[14] *CCBE Guidelines on…,* p. 5.
[15] In case of Polish Act on Protection of Personal Data Act it means though the need of verification whether a particular service provider is established in Poland or in the European Economic Area. If not, art. 47 and 48 of this Act should be applied.
[16] *CCBE Guidelines on…,* p. 7.

regulate this matter. CCBE remains as well that lawyers must control right to access to data stored by them in the cloud and security measures adopted by the service provider. Moreover, all the aspects of technical, organizational and legal security measures including proper documentation, back-up policies, recovery plan, monitoring and reporting schedule must be verified before the final decision about choosing a service provider is taken.

Another crucial issue is the one of termination of the contract. This matter must be checked before the contract is concluded. It is essential to know what would happen with the data processed in the cloud after termination of the contract. It may occur, that even if cloud computing service is no longer provided data is still processed in the could (in the service provider databases or in back-up databases). Looking at this problem from the perspective of lawyer obliged to keep the secret it is obvious that very weak point and very big danger for confidential data occurs in such case.

Last but not least, trust and transparency – values without which provision of the legal service would never be fully effective – should always be taken into consideration. If relation between lawyer and his client must be transparent, lawyer must also inform the client about the rules of providing legal aid. It means that lawyer should consider informing his future clients that the law firm uses cloud computing services[17]. Polish deontological and ethical codes[18] issued on the basis of the legal acts concerning solicitors and barristers oblige them not to disclose any kind of information related to the clients' case. It means, that use of the cloud computing in any case is not possible unless prior consent of the client is obtained. Furthermore, use of any other solution including electronic communication, applications used to manage all the data in the legal office, shared calendars and documents – these are all solutions that can be implemented only if clients' prior consent is obtained for their use.

4.2. Couple of remarks from outside Europe

Despite already mentioned guidelines of CCBE, lawyers seeking a piece of advice on how to use cloud computing in their legal practice may have insight in guidelines prepared by other chambers. Completing already presented recommendations, couple of general rules of code of conduct as it comes to use of technology may be indicated.

[17] CCBE Guidelines.

[18] See: Code of Conduct of Legal Advisor from 28.12.2010 http://kirp.pl/wp-content/uploads/2014/09/KERP-tekst-jednolity.pdf (binding till the 30.06.2015) and its new version that would enter into force on the 1.07.2015 http://kirp.pl/wp-content/uploads/2014/09/Uchwała_NKZRP_3_2014.pdf and Code of Conduct of Barrister text accessible at http://www.nra.pl/dokumenty.php.

Canadian Bar Association, highlights a general need for reasonable understanding of the technology and underlines that technology should be used with external help only if this help is provided by the entity having necessary proficiency[19].

Law Society of British Columbia, promotes an application of due diligence as it comes to use of third party service providers[20]. Due diligence in such case is for sure worth of considering. Taking into account a particular regime of providing the legal services and a number of risks connected with use of technology, lawyer should always bear in mind certain check list of provision to check and negotiate if necessary.

Law Society of South Africa brings attention to the point that "the use of cloud computing technologies is not inconsistent with a lawyers' ethical duties provided that lawyers should exercise due diligence before utilising a third-party service provider for confidential data storage or information processing in the cloud. In addition, a written agreement should be concluded that requires the service provider to establish and maintain measures that ensure the security of any personal information stored by the service provider as well as the protection of the integrity and confidentiality of client information"[21]. This recommendation could be applied step by step into the Polish legal system with no prejudice to the Polish legal requirements in the field of data protection.

The above mentioned are examples of rules can for sure be copied and applied by legal professionals not only in Poland. Taking into account their scope and scope of problem that arises when new technologies are used, the question may be asked if it is possible to use new solutions acting in full conformity with law. By the example of the cloud computing, it can be assumed that "The general consensus internationally is that the use of cloud computing architectures does not violate any ethical duty […] provided that reasonable care is taken effectively to minimize any risks to the confidentiality and security of client information […]"[22]. This statement is for sure a true one. Technology is not the obstacle in legal practice unless it is used with due diligence and the greatest care as it comes to making choice of particular solution.

[19] *Guidelines for Practicing Ethically with New Information Technology*, Canadian Bar Association, accessible on 10.03.2015 at http://www.cba.org/cba/activities/pdf/guidelines-eng.pdf.
[20] G. Hume, B. LeRose, P. Lloyd, S. Kuiack *Report of the Cloud Computing Working Group*, Appendix 1 – Due Diligence Guidelines, Law Society of British Columbia, 27.01.2012.
[21] *Guidelines on the Use of Internet-Based Technologies in Legal Practice,* Law Society of South Africa 2014, p. 10.
[22] *Guidelines on the Use*, Law Society of South Africa, 2014, p. 4-5.

5. Conclusions

Taking into account certain misunderstandings in application of the Act on Protection of Personal Data to the legal activity, challenges and risks strongly connected with use of technology and obligation to guarantee full confidentiality of data of the clients, lawyers should look for protective mechanisms in the data protection act. Incorrect identification of the Act on Protection of Personal Data as the act protecting secrecy becomes the basis for the difficult relation between processing of data and obligation to keep in secret everything that lawyers gets to know when providing legal service. Incorrect replacing data protection by the professional secrecy leads to situation in which data protected within the professional secrecy regime, is not protected by the personal data system. In the meantime, it should be kept in mind that data protection is in fact a procedure for handling the data, to ensure its security at the organizational and legal level and to guarantee its confidentiality, integrity and accountability. Therefore, professional secrecy and personal data protection system should be treated as complimentary pillars of full security and confidentiality, not as the systems excluding themselves.

The level of awareness of lawyers in the field of application data protection rules to their practice needs to change. Fortunately, the attention has already been brought to this problem in Poland thanks to the action taken by Polish Data Protection Authority. General Inspector for Data Protection announced that he would have start to control how do lawyers obey the data protection law and he started the series of training for lawyers in the field of data protection[23]. Building effective and well-functioning security system takes time and should be perceived as a long-lasting, but achievable process. The key point to understand is that making use of various services provided by the third parties means in fact entrusting data, often confidential and valuable, to them. The biggest challenge for the lawyer is to decide when use of third party service in done in favor of the client and in order to guarantee the highest standard of the service and when it is only a solution chosen by the lawyer to facilitate his work. It is undeniable that business is ruled by its own code of conduct, but legal professions with their particular ethical standards are not always submitted to these rules. The reason for that is very simple: legal professions need greater trust and transparency than other ones. It requires though greater care and diligence as it comes to the choice of how to provide a service and by what means.

[23] See: paper review with current Assistant Supervisor of the European Data Protection Supervisor from 26.07.2103 acting that time as General Inspector of Data Protection in Poland, Gazeta Prawna accessible on the 17.03.2015 at http://prawo.gazetaprawna.pl/artykuly/721357,giodo-zapowiada-kontrole-u-prawnikow.html.

Chapter 5

OPEN GOVERNMENT DATA: LEGAL, ECONOMICAL AND SEMANTIC WEB ASPECTS

Dino Girardi[1], Monica Palmirani[2]

[1] Ph.D. Candidate, Institute for Law and Informatics – University of Lapland, P.O. Box 122 - FI-96101 Rovaniemi, Finland, CIRSFID – University of Bologna, Via Galliera 3, 40121, Bologna, Italy, dino.girardi@ulapland.fi

[2] Professor of Legal Informatics, CIRSFID – University of Bologna, Via Galliera 3, 40121, Bologna, Italy, monica.palmirani@unibo.it

Keywords: *open data, public sector information, open government data, linked open data, transparency, personal data, licences, charging, business models, semantic web, interoperability, formats, standards, metadata.*

Abstract*: This paper is an overview on the Open Government Data (OGD) environment in the EU. It aims to point out the relevant legal issues together with the economic aspects arising from the disclosure and exploitation of OGD. Therefore, the paper highlights the noteworthy technological aspects related with the opening of OGD datasets. This survey is based on an interdisciplinary approach. Interdisciplinarity in the digital environment means that OGD should be considered as an integrated, interoperable and collaborative ecosystem. The main legislative source taken into account for the survey is the Directive 2003/98/EC on the re-use of public sector information as recently amended by the Directive 37/2013/EU.*

1. An Overview on Open Government Data

The concept of Open Data and specifically Open Government Data (OGD) refers to policies and practices of the States related to opening their datasets (constituted by Public Sector Information –PSI) and making them generally available for anyone free to access and re-usable for any lawful purpose.

The Open Knowledge Foundation – OKF[1] provides a definition of Open Data that is generally accepted and broadly used. As to the Open Definition "Open data is data that can be freely used, reused and redistributed by anyone – subject only, at most, to the requirement to attribute and sharealike"[2]. The Open Definition sets out in detail the requirements for "openness" in relation to content and data in the "Open Data Handbook"[3].

In the Open Government Data website[4] the OKF defines Open Government Data as follows:

- "open" means data that is open according to the Open Definition, as above explained.
- "government data" means data and information produced or commissioned by government or government controlled entities.

Referring to the EU Directive 2003/98/EC, Government Data is synonymous of Public Sector Information (PSI). The public sector bodies of the Member States "collects, produces, reproduces and disseminates a wide range of information in many areas of activity, such as social, economic, geographical, weather, tourist, business, patent and educational information"[5]. This information, recorded as documents, "constitute a vast, diverse and valuable pool of resources (datasets) that can benefit the knowledge economy"[6].

The same concept is clarified in the Open Data Handbook: "Open data, especially open government data, is a tremendous resource that is as yet largely untapped. Many individuals and organisations collect a broad range of different types of data in order to perform their tasks. Government is particularly significant in this respect, both because of the quantity and centrality of the data it collects, but also because most of that government data is public data by law, and therefore could be made open and made available for others to use"[7].

In this paper, reference to the Open Government Data (OGD) means Public Sector Information (PSI) datasets opened and disseminated as to the Open Data notion.

[1] The Open Knowledge Foundation –OFKN, trading as Open Knowledge, is dedicated to promoting the creation, sharing and application of Open Knowledge in the Digital Age. More detail about OFKN can be found at https://okfn.org/about/.
[2] http://opendatahandbook.org/guide/en/what-is-open-data/
[3] From the OFKN website: "This handbook discusses the legal, social and technical aspects of open data. It can be used by anyone but is especially designed for those seeking to open up data. It discusses the why, what and how of open data – why to go open, what open is, and the how to 'open' data". The full version of the handbook can be downloaded at: http://opendatahandbook.org/guide/en/.
[4] Open Government Data website http://opengovernmentdata.org/
[5] Recital (4), Dir. 2003/98/EC.
[6] Recital (2), Dir. 2013/37/EU.
[7] Open Data Handbook Documentation, Release 1.0.0 p. 4, http://opendatahandbook.org/guide/en/

The concept of OGD paradigm as a global phenomenon is based on several initiatives like the Obama's declaration[8] of 2009, the Tim Berners-Lee TED talk[9] in 2009 and the Cameron[10] letter in 2010. Therefore, in June 2013 the Open Data Charter[11] was approved by the G8 Members as a pillar strategic action for supporting transparency, accountability, participation, economic growth and innovation in society.

The 12th of December 2011 the European Commission, in order to achieve the aims as indicated in the Digital Agenda for Europe and to unlock the public data potential across Europe, has launched an "Open Data Strategy for Europe", enacting the so called "Open Data Package"[12]. The Open Data Strategy consists of:

1. a Communication on Open Data where the Commission presents its vision and policy on data re-use, including legislative, deployment and funding elements;
2. a proposal to revise the 2003 Directive on re-use of public sector information (Directive 2003/98/EC)[13]. The Directive has been recently amended by the "Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information"[14].

Recital (4) of the revised Directive point out the importance of adopting in EU common and harmonized open data policies encouraging "the wide availability and re-use of public sector information for private or commercial purposes". The circulation of the information "can play an important role in kick-starting the development of new services based on novel ways to combine and make use of such information, stimulate economic growth and promote social engagement".

The new Directive in recital (6) recognizes that some of the MS's "have been adopting ambitious open data approaches to make re-use of accessible public data easier for citizens and companies". As a result, in the same Recital the need of "a minimum harmonisation to prevent different rules in different Member States acting as a barrier to the cross- border offer of products and services, and to enable comparable public data sets to be re-usable for pan-European applications based on them is stated. A minimum harmonisation is also required to

[8] https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
[9] http://www.w3.org/2009/Talks/0204-ted-tbl.
[10] http://webarchive.nationalarchives.gov.uk/20130109092234/http://number10.gov.uk/news/letter-to-government-departments-on-opening-up-data/.
[11] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207772/Open_Data_Charter.pdf
[12] http://ec.europa.eu/digital-agenda/en/open-data-0
[13] http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive/psi_directive_en.pdf
[14] The official version of the Directive is available at this link: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0037.

determine what public data are available for re-use in the internal information market, consistent with the relevant access regime".

This paper is based on an interdisciplinary approach taking into consideration legal, economical, technological and semantic web aspects of OGD. The legal aspects of the survey consider transparency, accountability, data protection and licences. The economical value of OGD examines the issues related with charging of PSI and the need for developing sustainable Business Models for OGD. Finally, the paper highlights the noteworthy technological aspects related with the opening of OGD datasets in the Semantic Web like formats, metadata, linked open data and interoperability.

The following analysis is mainly based on the content and perspective of the above-mentioned PSI re-uses Directive.

2. Transparency, Right of Access to Information and Accountability

The Principle of Transparency has a constitutional basis and provides the fundamental legal framework for the administrative action and policy. The Transparency Principle ensures all the citizens the freedom of information and the right to consult or obtain information and data maintained by the Public Sector Bodies. So far Transparency has been granted under the national freedom of information regulations accordingly to the Principle of Access to the administrative acts and the Principles of Publicity of the acts[15]. Openness and availability of Public Sector Information are therefore ensured to citizens on the basis of the Right of Access.

The first 'freedom of information activists' were the enlightenment thinkers in Sweden and Finland who successfully promoted the adoption of Sweden's 1766 Freedom of the Press Act which establishes the principle of the openness of official documents and is widely considered to be the world's first access to information law. The right to access and use information were intrinsic to freedom of the press according to this constitutional law, which established a freedom to print in whole or in part extracts from *"correspondence, documents, protocols, judgments and awards* [produced by] *courts and government departments, our senior administrators and consistories or other public bodies ... which, when requested, shall immediately be issued to anyone who applies for them on penalty of the provisions following*

[15] Article 1, as to the Consolidated version of the Treaty on European Union and the Treaty on the Functioning of the European Union. http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2010:083:SOM:EN:HTML.
Italy: Law 241/90 on Administrative Procedure and Access to Administrative Documents: http://www.ictparliament.org/node/2040.
Finland: Act on Openness of Government Activities: ec.europa.eu/information_society/policy/psi/docs/pdfs/implementation/fi_trans_19990621.pdf.

paragraph". Documents should be provided "immediately" and the penalty foreseen is loss of office for the public official who fails to provide the documents or in any way obstructs their release[16].

Finland was part of Sweden when the first Act on the Freedom of Publishing and the Right of Access to Official Documents was enacted in 1766. Finland, as an Independent Republic, adopted the Act on Access to Information Law in 1951.

The right of access to information has developed significantly in recent years, with at least eighty countries worldwide currently having a dedicated legal framework for requesting and receiving information[17]. The right is also enshrined in at least fifty national constitutions.

In the OGD environment Transparency and at the same time Accountability of Governments and Public Entities are fundamental issues. Following this, Barack Obama in the speech he delivered when he was elected president of the United States for the first time opened the way to a new process in the field of democracy in the digital era. In the Memorandum for the Heads of Executive Departments and Agencies on the 21 January 2009, President Obama declared: "My Administration is committed to creating an unprecedented level of openness in Government. We will work together to ensure the public trust and establish a system of transparency, public participation, and collaboration. Openness will strengthen our democracy and promote efficiency and effectiveness in Government"[18]. In his Memorandum the President instructed the Director of the Office of Management and Budget to issue an Open Government Directive. The Directive was enacted on the 8 December 2009[19].

The three principles of transparency, participation, and collaboration form the cornerstone of an Open Government policy. From the Obama declaration we can read: *"Transparency promotes accountability and provides information for citizens about what their Government is doing. Information maintained by the Federal Government is a national asset. My Administration will take appropriate action, consistent with law and policy, to disclose information rapidly in forms that the public can readily find and use. Executive departments and agencies should harness new technologies to put information about their operations and*

[16] "The World's First Freedom of Information Act", published by the Chydenius Foundation (2006) available at: http://www.chydenius.net/pdf/worlds_first_foia.pdf.
[17] Some examples: Italy: Law 241/90 on Administrative Procedure and Access to Administrative Documents: http://www.ictparliament.org/node/2040. Finland: Act on Openness of Government Activities: ec.europa.eu/information_society/policy/psi/docs/pdfs/implementation/fi_trans_19990621.pdf.
[18] Memorandum for the Heads of Executive Departments and Agencies, SUBJECT: Transparency and Open Government, http://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment.
[19] http://www.whitehouse.gov/open/documents/open-government-directive.

decisions online and readily available to the public. Executive departments and agencies should also solicit public feedback to identify information of greatest use to the public".

Next, the EU Commission in 2011 with the Explanatory Memorandum of the Open Data Package invites the "European Parliament and the Council, within their respective responsibilities, to create the right framework conditions for the re-use of public sector information across the European Union, and to support the projects and infrastructures that can turn Europe's public data into a motor for innovation, growth and transparency". In particular as to the Memorandum "this will strengthen positive effect on the transparency, efficiency and accountability of governments and contribute to citizen empowerment"[20].

Subsequently in 2013, the G8 Open Data Charter Communication declared: "Open data can increase transparency about what government and business are doing. Open data also increase awareness about how countries' natural resources are used, how extractives revenues are spent, and how land is transacted and managed. All of which promotes accountability and good governance, enhances public debate, and helps to fight corruption. Transparent data on G8 development assistance are also essential for accountability"[21].

3. Open Government Data and Personal Data Legislation

Data Protection and the re-use of Public Sector Information in the European Union is a growing concern after the Commission has adopted the above-mentioned Open Data Package and the PSI Directive has been revised. Therefore, we should mention the proposal for a new Regulation on Personal Data Protection that Personal Data Protection that the EU is close to adopting.

In respect of processing personal data recital 11 of the revised Directive states: "the Directive should be implemented and applied in full compliance with the principles relating to the protection of personal data in accordance with Directive 95/46/EC". Therefore, the Member States should determine the conditions under which the processing of personal data is lawful. Furthermore, the recital highlights the Data Protection Directive principle which states that "personal data must not be processed further to collection in a way incompatible with the specified, explicit and legitimate purposes for which those data were collected".

[20] Proposal for a Directive of the European Parliament and of the Council Amending Directive 2003/98/EC on re-use of public sector information, http://ec.europa.eu/information_society/policy/psi/docs/pdfs/opendata2012/revision_of_PSI_Directive/proposal_directive_EN.pdf.

[21] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207772/Open_Data_Charter.pdf

It seems that the Directive has only partially taken into consideration the opinion issued by the European Data Protection Supervisor (EDPS) calling for data protection safeguards before public sector information containing personal data can be re-used[22]. The opinion of EDPS provides a detailed analysis covering many important aspects ranging from licensing, anonymization and transfer of data outside of the EU. Peter Hustinx, the EDPS, says: "The re-use of PSI containing personal data may bring significant benefits, but also entails great risks to the protection of personal data, due to the wide variety of data held by public sector bodies. The Commission proposal should therefore more clearly define in what situations and subject to what safeguards information containing personal data may be required to be made available for re-use."[23] In the opinion of EDPS, Open Data policies and Data Protection laws have similar objective: to create a fair environment for the circulation and the processing of data, but from PSI perspective, no personal data should enter in the open government data definition. This creates some weakness in the coordination among the two topics.

The EDPS calls for a proactive approach. As to the opinion of EDPS "it is crucial that public sector bodies take a proactive approach when making personal data available for reuse. A proactive approach would make it possible to make the data publicly available with the explicit purpose of reuse, subject to specific conditions and safeguards in compliance with data protection rules".

To ensure data protection compliance, EDPS recommends that the Commission develop further guidance on the data protection aspects of PSI re-use, primarily taking into account anonymization and licensing. The EDPS suggests the implementation of a template for adequate data protection clauses in licenses.

Finally, EDPS recommends that the EC Proposal of amending PSI Directive should:

- establish the scope of applicability of the PSI Directive to personal data more clearly;

- require that an assessment be carried out by the public sector body concerned before any PSI containing personal data may be made available for reuse;

- where appropriate, require that data be fully or partially anonymized and license conditions specifically prohibit re-identification of individuals and the reuse of personal data for purposes that may individually affect the data subjects;

---

[22] Opinion of the European Data Protection Supervisor on the "Open Data Package", http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-04-18_Open_data_EN.pdf.

[23] PRESS RELEASE EDPS/08/12, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2012/EDPS-2012-08_Open_Data_EN.pdf.

- require that the terms of the licence to reuse PSI include a data protection clause, whenever personal data are processed;

- where necessary consider the risks to the protection of personal data, require applicants to demonstrate (via a data protection impact assessment or otherwise) that any risks to the protection of personal data are adequately addressed and that the applicant will process data in compliance with applicable data protection law[24];

- clarify that reuse can be made contingent upon the purpose for which reuse is made, in derogation from the general rule allowing reuse for any commercial and non-commercial purposes;

In addition, the EDPS suggests that the Directive should:

- consider allowing costs of pre-processing (such as digitalization), anonymization and aggregation to be charged to license-holders where appropriate, and

- that the Commission develops further guidance, focusing on anonymization and licensing and consult the WP29[25] in this regard.

Concerning the anonymisation of OGD the WP29 has recently adopted the Opinion 05/2014 on Anonymisation Techniques (10 April 2014). In its opinion the WP 29 "acknowledges the potential value of anonymisation in particular as a strategy to reap the benefits of 'open data' for individuals and society at large whilst mitigating the risks for the individuals concerned"[26].

The revised Directive hasn't ruled on this specific issue of protection of personal data leaving the decision to the MS's and generically referring to the Data Protection Directive into force.

In regards to *de lege ferenda,* the data protection reform package is aimed at building a single and comprehensive set of data protection rules for the EU. The issue of Open Data has no specific provision in the Regulation proposal[27]. Nevertheless, in the proposal we can find provisions on central thematic like privacy by design, privacy by default and the right to be

[24] In this respect see: EVPSI & LAPSI Final Meeting Turin, 9-10/7/2012 Eleonora Bassi University of Turin. In this work are indicated the recommended tools in order to fulfil the EDPS purposes such as: PETs, Privacy by Design, Anonymisation, Privacy Policies, PIA, Codes of Conduct, Guidelines, Anonymisation by Default. www.lapsi-project.eu.

[25] WP29 recommend to adopt a case by case approach "in order to strike the balance between the right to privacy and the right to public access" (Opinion 7/2003, wp 83). WP29 (Working Party 29) was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 14 of Directive 97/66/EC http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp83_en.pdf

[26] The Opinion on Anonymisation Techniques adopted by WP29 is available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[27] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011&from=EN.

forgotten that will have a significant impact to OGD (and also Big Data) policies and legislation.

Regarding the right to be forgotten, the recent decision of the European Court of Justice in the case-law Google v. Costeja[28] clearly states the existence of the right of a person to see personal data correctly represented according to the veracity of the facts and the context. With regards to OGD, this concept means that opening datasets containing personal data requires that the Public Administrations constantly update the dataset according to the current circumstances. This task requires a good deal of the Public Sector resources. The request to erase or alter information is managed by each MS differently: the data may be deleted at the source, i.e. from storage, or the data may be removed from the indexing in the search engine. The Open data paradigm requires any search engine be open and that the information is indexed to permit wide sharing of information on the Semantic Web. Therefore, the right to be forgotten raises this new, and critical, issue in light of our understanding of the broad and widely distributed information in the Open Data environment.

4. Government Data and Licences

The legal conditions under which PSI are made available is considered by the revised Directive at Recital 26 "In relation to any re-use that is made of the document, public sector bodies may impose conditions, where appropriate through a licence, such as acknowledgment of source and acknowledgment of whether the document has been modified by the re-user in any way". The revised Article 8 of the Directive leaves the public sector open to "allow re-use without conditions". Therefore, public sector bodies, as to Recital 26 and Article 8 of the Directive, may impose "where appropriate" conditions for the re-use of PSI "through a licence" placing "as few restrictions on re-use as possible". Accordingly, some Member States have established their own Open Data Licence for PSI re-use like, the UK[29], Italy[30] and in Finland the National Land Survey[31]. The EU has itself adopted the European Union Public Licence (EUPL)[32]. Some Countries has adopted the ODL (open database license)[33] published by the Open Data Common. This licence agreement imposes the limitation of *share-a-like* causing sometime a barrier to the economic re-use of the datasets.

[28] http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
[29] http://www.nationalarchives.gov.uk/doc/open-government-licence/version/2/.
[30] http://www.formez.it/iodl/.
[31] http://www.maanmittauslaitos.fi/en/NLS_open_data_licence_version1_20120501.
[32] https://joinup.ec.europa.eu/software/page/eupl/licence-eupl.
[33] http://opendatacommons.org/licenses/odbl/

Furthermore, the revised Directive at Recital 26 encourages Member States to use open licences available online "relying on open data format" "(…) which grant wider re-use rights without technological, financial or geographical limitations". This "should eventually become common practice across the Union".

The Creative Commons Licences CC-BY 4.0 and CC-BY-SA 4.0 are a practical option for publishing both data and content. The release 4.0 package of CC includes the *sui generis* right that is the best way to protect dataset according with the European Directive 2004/48/EC and related Statement 2005/295/EC and Directive 96/9/EC. The OFKN has marked, *inter alia*, CC-BY 4.0 and CC-BY-SA 4.0 as conformant[34] with the principles set forth in the Open Definition[35] In between numerous examples of publication under the Creative Commons Attribution 4.0, we can mention as an example the Finnish Meteorological Institute's open data service[36]. The issue of licences is more essential after the revision has extended the scope of Directive 2003/98/EC "to libraries, including university libraries, museums and archives" as to Recital 14 of the Directive 2013/37/EU.

Within this framework, we should mention as an example Europeana[37] (Europe's digital library) that releases its metadata into the public domain using CC0. However, this decision of Europeana to impose to every contributor the CC0 is disputable. The CC0 is a waive license, and it is contrary to the moral right that is inalienable in Europe. Moreover, an open government dataset is inalienable proprietary of the public administration (like beaches, soil, etc.) and the statement included in the paragraph 2 of the universal CC0 "To the greatest extent permitted by, but not in contravention of, applicable law, Affirmer hereby overtly, fully, permanently, irrevocably and unconditionally waives, abandons, and surrenders all of Affirmer's Copyright and Related Rights" is not applicable by any employee of the public administration. This is a great dilemma especially for the cultural heritage material that is proprietary of the patrimony of a national State. Secondarily, these considerations uncover a further problem: how to conciliate so large a variety of licenses in case the market needs to mash-up dataset for producing commercial product, service and application. This topic is unresolved and it is one of the most important legal barriers to the success of a real business model of the open government data[38].

[34] http://opendefinition.org/licenses/.
[35] Read more about the Open Definition at: http://opendefinition.org/od/.
[36] http://en.ilmatieteenlaitos.fi/open-data-licence.
[37] http://www.europeana.eu/portal/.
[38] M. Palmirani, M. Mockus, *Open Government Data Licensing Framework* [in:] *Electronic Government and the Information Systems Perspective,* A. Kő, E. Francesconi (eds.) Fourth International Conference, EGOVIS 2014, Valencia, Spain, September 1-4, 2015, Proceedings, Springer, 2015.

5. Economical Value and Business Models for Open Government Data

The Communication of 2011 of the European Commission to the European Parliament "Open data an engine for innovation, growth and transparent governance" has an emblematic and challenging heading: "Turning public data to business opportunities: new services and economic growth"[39].

As referred to above, the PSI is the single largest source of information in Europe. The Open Data Package included evidence in a careful and detailed survey in order to show the economic opportunities arising from the exploitation of Government Data.

The European Commission believes that "overall economic gains from opening up this resource could amount to € 40 billion a year in the EU. Opening up public data will also foster the participation of citizens in political and social life and contribute to policy areas such as the environment".[40] This information has a significant - currently untapped - potential for re-use in new products and services and for efficiency gains in administrations.

A recent study carried on by Graham Vickery[41] and commissioned by the EC estimates the total public sector information related market across the EU in the year 2008 at Euro 28 billion and in 2010 at 32 billion Euro. The study indicates that the overall economic gains from further opening up public sector information by allowing easy access are at around 40 billion Euro a year for the EU27. The aggregate direct and indirect economic impacts from PSI applications and use across the whole EU27 economy would be in the order of Euro 140 billion annually. As to the Vickery study, the average growth rate in PSI-related markets is 7%. The total direct and indirect economic impact of PSI reuse is from 70 up to 140 billion of Euro. Finally, the welfare gains from to marginal cost pricing of the PSI will be 40 billion Euro.

Hal Varian, Professor of Information Sciences, Business, and Economics at the University of California at Berkeley and Chief Economist, Google maintains that "the ability to take data—to be able to understand it, to process it, to extract value from it, to visualize it, to communicate it—that's going to be a hugely important skill in the next decades, not only at the professional level but even at the educational level for elementary school kids, for high school kids, for college kids. Because now we really do have essentially free and ubiquitous

[39] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52011DC0882.
[40] Communication on Open Data, http://ec.europa.eu/information_society/policy/psi/docs/pdfs/directive_proposal/2012/open_data.pdf.
[41] Search on the web: Review of recent studies on PSI re-use and related market developments, G. Vickery, August 2011.

data. So the complimentary scarce factor is the ability to understand that data and extract value from it."[42]

The main issue arising from the revision of the Directive and affecting the economic value of datasets is the principles governing charging regulated in Article 6. The Directive in Article 6.1 lays down a charge, applying to all, for public sector data re-use in the EU, except the situations specified in Article 6.2: "public sector bodies may charge no more than the marginal cost of reproducing, providing and disseminating the documents". Nevertheless, article 6.2 of the Directive expressed the possibility "to sell" open government data reflecting "marginal costs incurred for their reproduction, provision and dissemination" along with "a reasonable return on investment".

The policy of lowering charges has been supported by researches and by the outcome of public consultations conducted by the Commission [43]. A series of case studies on public sector bodies that moved from full cost recovery to a marginal costs system show that the move not only increased re-use, but also benefited the public sector bodies concerned[44].

Heli Koski[45] from the Research Institute of the Finnish Economy has recently carried on a study about marginal cost pricing of PSI [46]. Assessing the performance of 14,000 firms in the architectural, engineering and related technical consultancy sectors, located in 15 different countries, the study analyses the effect of maximum marginal cost pricing for geographical PSI on the firms' growth performance during the years 2000–2007. The conclusions that Koski has reached are strongly supporting free data re-use.

This "reasonable return on investment" provision in the PSI Directive opens up an unexpected scenario for a business model based on the free circulation of knowledge not reflecting the OGD concept of datasets available free of charge[47].

However, the scientific research on business model (BM) of OGD is still scarce[48]. Therefore, the network economy is still facing a lack of studies that analyse and describe a suitable BM archetype for OGD.

---

[42] Hal Varian on how the Web challenges managers http://www.mckinsey.com/client_service/business_technology
[43]Commission staff working document SEC(2011) 1552 final; https://ec.europa.eu/digital-agenda/en/news/commission-notice-guidelines-recommended-standard-licences-datasets-and-charging-re-use.
[44] Study on 'Pricing of Public Sector Information', Deloitte consulting and others, June 2011.
[45] Does Marginal Cost Pricing of Public Sector Information Spur Firm Growth?', Heli Koski, The Research Institute of the Finnish Economy. http://www.etla.fi/files/2696_no_1260.pdf.
[46] About Principles governing charging see further on paragraph 3.2
[47] Monica Palmirani, Michele Martoni, Dino Girardi - Open Government Data Beyond Transparency in: Andrea K″o Enrico Francesconi (Eds.) Electronic Government and the Information Systems Perspective Third International Conference, EGOVIS 2014 Munich, Germany, September 1-3, 2014 – Proceedings.
[48] Eight Business Model Archetypes for PSI Re-Use by Osella – Ferro,www.w3.org/2013/04/odw/odw13_submission_27.pdf; Open growth Stimulating demand for open data in

In our opinion, an appropriate and applicable BM archetype for Open Data should distinguish two different models: one for Enterprises and NPO's and one designed for Public Sector Bodies. Considering a BM archetype for Enterprises it basically requires to describe differences and peculiarities between those using OGD as core business and those using OGD as a complementary business. Nevertheless, in our opinion it is of fundamental importance to develop a sustainable BM tailored for Public Sector Bodies.

Thinking from a research point of view, the analysis for developing a sustainable Business Model archetype for OGD should consider for instance solutions regarding: the analysis of the possible re-use and exploitation of available datasets on a large scale not only for political purposes (transparency and accountability); the implementation of back up option in case of a luck of delivering of data; the analysis of the quality of data (i.e. punctual, timely, complete, statistics); the accessibility for the end consumer; personal data and copyright issues; the consistency with the original purposes that have enabled the opening of the datasets; the benefits and the value creation for the Public Sector Bodies and the whole society.

The BM should primarily consider the following budgeting components:

- the expenditures related with the operational costs for collection, production, digitalization, manipulation, processing, storage, and dissemination of the datasets;

- consequently, the budgeting components associated with the expected revenue streams for the Public Sector Bodies like charges and tax revenue;

- additionally, the so-called indirect benefits and the social benefits arising for the exploitation of OGD, whenever they can be monetized.

Finally, the BM should describe two archetypes designed for public sector bodies that are required to "charge PSI at marginal cost" and one for those who are "required to generate revenue". In respect of the latter model, we should recall Article 6 "principles governing charging, that at point 2 reads: "paragraph 1 shall not apply to the following:

(a) public sector bodies that are required to generate revenue to cover a substantial part of their costs relating to the performance of their public tasks;

(b) by way of exception, documents for which the public sector body concerned is required to generate sufficient revenue to cover a substantial part of the costs relating to their

---

the UK – by Deloitte's and The Open Data Institute, http://www2.deloitte.com/content/dam/Deloitte/uk/Documents/deloitte-analytics/open-growth.pdf; Open data business models, by Jeni Tennison, www.theodi.org; D. Girardi, M. Palmirani, *Legal Issues and Economic Exploitation of Open Government Data*, "Jusletter IT" 15. Mai 2013; C. Bonina, New business models and the value of open data: definitions, challenges and opportunities, http://www.nemode.ac.uk/wp-content/uploads/2013/11/Bonina-Opendata-Report-FINAL.pdf; Magalhaes, Roseira, Manley, *Business models for open government data*, opendata500.thegovlab.org/files/Business_Models_for_OGD.pdf.

collection, production, reproduction and dissemination. Those requirements shall be defined by law or by other binding rules in the Member State. In the absence of such rules, the requirements shall be defined in accordance with common administrative practice in the Member State;

(c) libraries, including university libraries, museums and archives. Finally, "Where charges are made by the public sector bodies referred to in point (c) of paragraph 2, the total income from supplying and allowing re-use of documents over the appropriate accounting period shall not exceed the cost of collection, production, reproduction, dissemination, preservation and rights clearance, together with a reasonable return on investment".

6. Technological issue for Open Government Data in the Semantic Web

Finally, from the previous paragraphs we have understood that Open Government Data is a global phenomenon adopted at political level by numerous public administrations. Therefore, the EU Commission have encompassed this crucial topic in the Digital Agenda as one of the main pillars in order to develop a Digital Single Market[49]. OGD implies a new cultural approach for implementing transparency, sharing of knowledge, participation and cooperation. OGD are also the essential instrument for supporting and developing a digital economy and for improving the quality of the life of the citizens. It is also a great instrument for fighting corruption, criminality, and bad administrative practices inside of the public administration. OGD also requires managerial competences and engineering skills in order to produce a culture of quality of data since the original digital information system inside the public administration requires reengineering.

Nevertheless, is indubitable that without technology principles OGD is only a manifesto. Therefore, we should comment on the need of technological methodologies, which enable the opening, and dissemination of reusable public datasets to ensure their interoperability in the Semantic Web. As in the Open Data Handbook,[50] "interoperability denotes the ability of diverse systems and organizations to work together (inter-operate), to cooperate, to exchange information automatically, to interact seamlessly anywhere, anytime on the base of common rules". In the case of Open Data, interoperability is the ability to interoperate - or intermix - different datasets. "The core of a "commons" of data (or code) is that one piece of "open" material contained therein can be freely intermixed with other "open" material. This interoperability is key to realizing the main practical benefits of "openness": the dramatically enhanced ability to combine different datasets together and thereby to develop more and better

[49] http://ec.europa.eu/digital-agenda/en/our-goals/pillar-i-digital-single-market.
[50] http://opendatahandbook.org/.

products and services. Providing a clear definition of openness ensures that when you get two open datasets from two different sources, you will be able to combine them together, and it ensures that we avoid our own 'tower of babel': lots of datasets but little or no ability to combine them together into the larger systems where the real value lies."[51]

Recital (20) of the revised Directive reads: "To facilitate re-use, public sector bodies should, where possible and appropriate, make documents available through open and machine-readable formats and together with their metadata, at the best level of precision and granularity, in a format that ensures interoperability". As to Article 2.6 of the PSI Directive a format is 'machine-readable' when the "file format is structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure". Additionally, Article 2.7 defines 'open format' as a "file format that is platform-independent and made available to the public without any restriction that impedes the re-use of documents".

In the light of the legal provisions from a technical perspective there are four main principles to consider:

i) Open format;

ii) Metadata;

iii) Ontology;

iv) Persistent URI.

Open format. Besides the legal definition in computer science open format also means well documented, easily applicable, no proprietary and neutral respect the technology environment. Examples of open formats are: CSV, JSON, XML, RDF[52].

Metadata. The dataset itself is not enough for implementing the reusability. It is also necessary to explain the semantic of the data. For this reason, two more elements are necessary: metadata and ontology. Metadata is machine understandable information on the dataset, understandable in the Semantic Web platform[53]. Metadata are classified according to standard vocabularies to facilitate searching and interoperability. Without metadata, the dataset is only a list of values without meaning and contextualization. Article 2.8 and Article 6 of the Directive clarify that "both the format and the metadata should, in so far as possible, comply with formal open standards", "…which has been laid down in written form, detailing specifications for the requirements on how to ensure software interoperability". So, it is important to have them

[51] http://opendatahandbook.org/guide/en/what-is-open-data/.
[52] For an exhaustive analysis about open format see: http://opendefinition.org/ofd/.
[53] http://www.w3.org/Metadata/.

jointly with the dataset for supporting a correct re-use according to the intention of the author. Without precise metadata the re-use can produce corrupted results and the datasets are prone to the manipulation, mystification and wrong interpretation. One of the most important methodologies for providing metadata is RDF (Resource Description Framework) that permits to make assertion on the main source using triple method: subject (dataset), predicate (relationship), object (attribute). One typical assertion is to define creator, date of creation, subject of the dataset. An example is the following that states Palmirani is the creator of the dataset1 using Dublin Core[54] vocabulary:

```
<rdf:RDF
  xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"
  xmlns:dc="http://purl.org/dc/elements/1.1/">
   <rdf:Description rdf:about="http://example.org/dataset1">
   <dc:title>dataset1 OGD</dc:title>
   <dc:creator>Monica Palmirani</dc:creator>
</rdf:RDF>
```

Ontology. As paradigmatic example of ontology we can refer to DCAT[55] that "is an RDF vocabulary" developed by W3C "designed to facilitate interoperability between data catalogues published on the Web". EUROVOC[56] is a multilingual, multidisciplinary thesaurus covering the activities of the EU, the European Parliament in particular. Besides the datasets, sometimes it is fundamental to annotate also the schema, the vocabulary and taxonomies. ADMS[57] is a specific application of DCAT, used to describe *semantic assets* defined as highly reusable metadata (e.g. xml schemata, generic data models) and reference data (e.g. code lists, taxonomies, dictionaries, vocabularies) that are used for eGovernment system development. In this way, we can describe the dataset (e.g., XML), the metadata of the dataset (e.g., DCAT) and finally also the vocabulary or schema for interpreting the dataset (e.g., with ADMS).

Computational Ontology. Computational ontology is the abstract representation a specific domain using classes, attributes, relationships[58]. A computational ontology sets up a semantic modelization of the reality that, if it is shared among a community, can create a common meaningful map of concepts. Using axioms, it is possible to create inferential rules among the objects connected with the classes of the ontology. In order to exemplify the concept: "if the

[54] http://dublincore.org/ Dublin Core is one important vocabulary for assigning metadata to the sources in the Web.
[55] http://www.w3.org/TR/vocab-dcat/.
[56] http://eurovoc.europa.eu/.
[57] http://www.w3.org/TR/vocab-adms/.
[58] http://tomgruber.org/writing/ontology-definition-2007.htm

dataset is created by Palmirani and if Palmirani belongs to the University of Bologna, then the dataset is published by University of Bologna".

Persistent URI. The possibility to have persistent, meaningful, semantic URI, http based for each different web resource is a fundamental principle in order to make valid the RDF and the ontology statements. Using these ingredients, it is possible to create an interoperable infrastructure capable to be connected with the Semantic Web constellation of data. Tim Berners-Lee[59] defines the Semantic Web as "a web of data that can be processed directly and indirectly by machines"[60]. "The Semantic Web is a Web of Data — of dates and titles and part numbers and chemical properties and any other data one might conceive of. The Semantic Web stack[61] (URI, XML, RDF, OWL, Logic, Proof, Trust) provides a complete environment where the data are reference-able, modelled, enriched, inferenced and detected with provenance metadata. Additionally, Linked Open Data[62] methodology provides the best way to publishing the datasets in Semantic Web context. Linked Open Data publication requires four rules:

1. Provide a persistent URI for each dataset;
2. URI http based;
3. Use RDF metadata connected to the dataset;
4. Re-use other ontologies.

Linked Open Data is a best practice worldwide accepted about open data, however it is not easy to implement it, so it is possible to apply this paradigm step by steps following, gradually, the method of the Tim Berners Lee's 5 stars[63]:

1. Provide dataset on the web with open license;
2. Provide dataset in machine-readable open format;
3. The open format should be non-proprietary;
4. Link the data to RDF metadata;
5. Link the data to other data available in the Linked Open Cloud[64].

Linked Open Data attempt to resolve the interoperability dilemma of the Web of Data. However, it is difficult to share the same understanding of a concept equally worldwide. The perception of the realty is different by each person, so we should add a level of provenance to the interpretation. As an example, the legal dataset is fundamental to permit multiple

[59] http://www.w3.org/People/Berners-Lee/
[60] T. Berners-Lee, J. Hendler, Ora Lassila (May 17, 2001),"The Semantic Web". *Scientific American Magazine*. Retrieved March 26, 2008.
[61] https://en.wikipedia.org/wiki/Semantic_Web_Stack.
[62] http://www.w3.org/wiki/LinkedData.
[63] http://www.w3.org/DesignIssues/LinkedData.html.
[64] http://lod-cloud.net/.

annotations of the same dataset with different licenses and different metadata datasets. In this scenario the risk is to have too much dataset without the corresponding metadata and semantic that is fundamental for expressing the level of integrity and authority. The inferential process generated new knowledge derived by the datasets, but the outcomes are valid only if the premises are well supported by the evidence of accuracy, truthfulness and authenticity. For this reason ontology like PROV-O[65], devoted to tracking the provenance of the data, is fundamental for guaranteeing the validity over time of the information and avoid manipulation of reality. Another emerging topic in this respect is the issue concerning the long-term preservation of the dataset not only as historical memory of the cultural heritage of a nation, but moreover for archiving in safe and secure way the dataset produced by the public administration.

7. Conclusions

In the light of the current European Union panorama, so far, OGD policies have mainly met a political and social function in respect of transparency and accountability of Governments and public entities. The commercial value of OGD is so far evident in countries and regions that have adopted ambitious and strategic projects for the exploitation of OGD at any level (i.e. UK, Italy, Austria, Germany, Finland, Estonia). On the other hand, in part of the MSs Open Government Data, policies are still in early infancy.

The current EU scenario is like an archipelago with a lack of bridges connecting OGD policies and strategies in different Member States. The revised Directive on PSI re-use has established a minimum harmonisation to prevent different rules in different Member States acting as a barrier to the cross- border offer of products and services, and to enable comparable public data sets to be re-usable for pan-European applications. Nevertheless, the implementation of the Directive in the MS legislation is developing slowly, and OGD policies are left to the political decision of a single Member State. As a result, there will most likely be weak harmonisation.

This paper has pointed out the need for an interdisciplinary approach in order to enable a wider exploitation of OGD for commercial and non-commercial purposes. In our opinion, Open Government Data in EU should be considered as a harmonized, integrated and interoperable ecosystem. Citizen, users, public entities, NPO's and private enterprise should work, collaborate and especially cooperate. These various players, with their own special roles and skills, should cooperate in an interactive dialogue in order to prove and exploit the potential of

[65] http://www.w3.org/TR/prov-o/.

Open Government Data. The availability of more OGD is not only a method for publishing data for the external end-users, it is also a great instrument for the cooperation between public sector bodies that often are not able to integrate the information systems, and to provide efficient services to citizens and enterprises. Secondarily, the paradigm of OGD is also a way for enhancing the internal communication among departments of the same public sector bodies that are otherwise not consciousness of the wide repository of information available. OGD creates a new methodology of work inside and outside of the public administration and produces an innovative flow of data supporting the digital economy and enhances cooperation between the private and public sector preparing the next step of the Internet of the Thing[66]. This reinforces the concept that OGD is beyond the notion of transparency and accountability and would be one part of a real modern democracy in the network society[67].

[66] The Internet of Things—A survey of topics and trends, Andrew Whitmore, Anurag Agarwal, Li Da Xu, Springer, 2014.

[67] M. Palmirani, M. Martoni, D. Girardi, *Open Government Data Beyond Transparency* [in:] *Electronic Government and the Information Systems Perspective,* A. K˝o, E. Francesconi (eds.), Third International Conference, EGOVIS 2014 Munich, Germany, September 1-3, 2014 – Proceedings.

Chapter 6

ABUSES OF DOMINANT ICT COMPANIES IN THE AREA OF DATA PROTECTION

Aleksander Wiatrowski

Ph.D. Student, University of Lapland, Institute for Law and Informatics, Yliopistonkatu 8, 96300 Rovaniemi, Finland, awiatrow@ulapland.fi

Keywords: *Dominance, data protection, privacy, Microsoft, Facebook, Google*

Abstract: *The existence of dominant companies such as Microsoft, Google, Facebook, etc. result in a dangerous situation in terms of abuses of data protection and data security legislation. It is important to specify the term "dominant" or "dominance" as, in my opinion, the existing definition from a competition law perspective does not apply to the situation concerning privacy and data protection. So far law has not presented any other sufficient way to describe "dominance".*

1. Introduction

In my dissertation[1], Abuses of Dominant ICT Companies in the Area of Data Protection, I am focusing, as stated, among other issues, on dominant companies. I am definitely not interested in the actions of smaller and less significant entities, from the economic and legal point of view.

This paper underlines the reason for this choice. Why is dominance so important? I want to prove, in my dissertation, and here, that the companies selected by me, by the fact they are dominant, have a significant and major impact on legal and factual actions in the wide area of data protection and privacy.

Microsoft, Facebook, Google are so huge and influential that they are already known for abusing their position in numerous cases. Even more important is the fact that their economic situation, as well as global position allows them to easily pay all the fines against them. So far

[1] By finishing the dissertation in Finland one gains the doctoral degree and the title of doctor in Finnish called "tohtori", more about the regulations concerning dissertation at University of Lapland: http://www.ulapland.fi/InEnglish/Research/Graduate-School/Dissertation-and-public-examination (access June 2015).

it seems that the tools countries and organizations all over the world have at their disposal, are not enough to stop dominant companies from their actions, which sometime balance on the verge of what is legally allowed and very often are simply illegal.

Nowadays when the European Union is working on new solutions, such as new data protection regulation, it may seem that we should just sit and wait. On the other hand, we can examine the example of Finland which already has developed more efficient and complex legislation. But even with this, dealing with Facebook or Google is extremely difficult.[2]

I would like to present dominance and super dominance, explain why dominant companies are in a very comfortable position, and why focusing on them is so important in understanding the threats to privacy and data protection and data security.

Where is the competition law in this topic and in my dissertation? Why am I focusing so much on competition law? These are the questions which needed to be answered at the beginning.

Dominant companies and dominant entities, or to be more exact, the whole concept of dominance comes directly from the competition law dictionary. Both in my dissertation and in this paper I focus on dominant companies or entities because the bigger the amount of power on the market, a subject has, the bigger an abuser it can potentially be.

Other than the fact that competition law interests me, it is also one of the oldest branches of law dealing with powerful, often international subjects. Therefore, provisions are more complete, lawyers more experienced, and there are more cases to learn from. If lawyers can deal with dominant subjects when it comes to business related cases, abusing market position and copyrights, then maybe in looking for solutions in the area of data protection and privacy we could use the experience of competition lawyers.

As my area of interest is at first data protection and privacy I want to use competition law definitions literally. Especially because competition law is known for lacking precise definitions or definitions at all.[3]

I would like to explain how common legal understanding of the term "dominance" or "dominant", coming from competition law, may not be sufficient in case of my topic. There are several criteria which I will present, to explain how different the companies are that I have chosen for my topic from those which are usually called "dominant" or "super dominant". There is definitely the place for new term, like "global dominance" or "absolute dominance".

---

[2] R. Aarnio, *Data Protection Reform – are we ready? - 25 years of Data Protection in Finland*, presentation from KnowRight2012, Helsinki.

[3] Example: Monopoly de jure, monopoly de facto, dominance.

One thing should be taken under strong consideration. It is not only about "dealing" with companies or with the problems caused by them. It is definitely not only about creating aggressive legislation to have tools to fight them. It is also, and maybe mostly about convincing them that legal way is the way to go. This may convince those companies to "behave", or rather should I say, limit their abuses. After exposing many global ICT companies' huge contribution to mass surveillance[4], for example Microsoft decided to take a completely different approach - "Microsoft experiences will be unique as they will reason over information from work and life and keep a user in control of their privacy." It is stated that Microsoft is helping put users in control in three ways: by building privacy into policies and practices, building privacy into products and by advocating laws and legal processes that keep people in control.[5]

The dominance is an underrated factor in dealing with abuses in all legal areas, not only privacy or data protection. It deserves a proper explanation to underline the issue. I want to explain that in the topic of my dissertation "Abuses of Dominant Companies in the Area of Data Protection", part "Dominant Companies" may be more important than "Abuses". Of course together, it highlights the whole idea, but when the fact of existence of abuses is well known, the influence and importance of dominance is less considered.

2. Non-legal Dominance?

During my short academic experience as a doctoral student I noticed interesting phenomenon. Whenever I mention the topic of my dissertation, Abuses of Dominant ICT Companies in the Area of Data Protection, the reaction is always the same – "You are writing about Google, Facebook etc." It is on the one hand helpful, as helps me jump right into the core of the discussion. On the other hand, it means only one thing. Lawyers have one understanding of the term "dominance". It is the competition law "dominance".

Why do I think it is an issue? Mostly because it somehow simplifies the complexity of the problem in the area of data protection and privacy, and at the same time it complicates it. Competition law without really explaining what dominance is, creates a lot of criteria which are not helpful for the purpose of my dissertation. In it I would like the term "dominance" to be kept simple and sharp.

[4] J. Brustein, *The Companies' Lines on Prism*, June 07, 2013, http://www.businessweek.com/articles/2013-06-07/the-companies-lines-on-prism (access June 2015).
[5] Data Privacy Day 2015 – Putting people in control, http://blogs.microsoft.com/on-the-issues/2015/01/28/data-privacy-day-2015-putting-people-control/ (access June 2015).

3. Dominance in Competition Law

Naturally whenever we use the terms "dominance" or "dominant position" we should and we do think about competition law. That means with the topic "Abuses of Dominant Companies in the Area of Data Protection" the first thing that comes to mind is the connection between Competition Law and Legal Informatics or IT Law.

It is a right guess, and it is at the same time a wrong one. "Dominance" definitions taken from competition law are not even complete or if we want to look for them in legislation, there are none.

What is the "dominance" taken under discussion in almost every publication concerning antitrust law or competition law? Without defining this term, or without quoting relevant provisions it is pointless to discuss. Of course it may seem that at this point everything has been already said and defined. Yet, there are still plenty of problems and issues. Even though I am not exactly interested in traditional competition law, this way of understanding "dominance" is what I need to include in this paper.

The prohibition on abuse from article 102 TFEU[6] only applies to the conduct of companies with a dominant position – assessment of dominance is an essential requirement for its application. The first problem is that the article, or the whole Treaty on the Functioning of the European Union does not explain what "dominance" is. Single company dominance, the one I am mostly interested in, was defined early by the European Court of Justice (ECJ) in *United Brands*[7] and *Hoffmann-La Roche*[8] cases as "a position of economic strength enjoyed by an undertaking which enables it to prevent effective competition being maintained on the relevant market by affording it the power to behave to an appreciable extent independently of its competitors, customers and ultimately of its consumers."[9] Even this definition, widely accepted and used, raises serious uncertainties: the concepts of economic strength or independence ignore the fact that in most markets, no company is truly independent and there is no indication of which degree of economic strength or independence must be achieved.

Additionally, in competition law, it is required to look for a relevant market. It can be a product market or a geographical market and it is important to assess the time of dominance. In

[6] Treaty on the Functioning of the European Union.
[7] Case 27/76, *United Brands Co i United Brands Continental BV* [1979] para. 207.
[8] Case 85/76, *Hoffmann-La Roche La Roche & CoAG* [1979], para. 461.
[9] Case 322/81 *Nederlandsche Banden-Industrie Michelin NV v. Commission* [1983] ECR 3461 para. 30, see also Case 27/76 *United Brands Co. v. Commission* [1978] ECR 207 para. 65; Case 85/*76 Hoffmann La Roche v. Commission* [1979] ECR 461 para. 38.

case of super dominant companies, it is also a part of discussion, yet in my opinion competition law simplifies the problem.

Competition law is, even if with some understatements, focusing on economic point of view. Where and when the company is dominant, what is the market share, is the company independent, has the consumer alternative and so on.

The dominance I am interested in is different. Of course the company has to be dominant presently. It has to be a global and has multinational position. Obviously the company has to have strong market position in relation to data processing.

a. Super Dominance

From time to time the term "super dominance" or "super dominant position" has appeared in case law. It was popularized in *Microsoft* case and referred to Microsoft's share of more than 90% on the operating systems' market. Before that, it was presented for the first time in the *Tetra Pak*[10] case and confirmed later in the *Compagnie Maritime Belge* case in the opinion of Advocate General Fennelly. He described it as a "position of such overwhelming dominance verging on monopoly" that it would give rise to "particular onerous special obligations".[11]

The term "super dominance" may seem to very accurately and rightly describe position and situation of the companies I have chosen for my dissertation and this paper. Unfortunately, in fact it is only a clever way of saying that a company has a massive advantage on the particular market. What is more, this concept has not yet been specifically referred to by the Commission or the European Courts – with one exception of *Microsoft* case.[12]

I like this term very much, but unfortunately because of its nature it is not really useful to me. I am not seeking for a definition focused on market position *per se*.

Yet, I am mentioning it. The first reason is because I want to emphasise how, for competition law, dominance has become a way of describing economic position. The second reason is because I hoped to find a term, to name the situation in the area of data protection and data security. It is not super dominance, but the appearance of such terms in case law shows that sometimes there is a need to create unusual, I would even say flashy names.

[10] Case C-333/94 P, *Tetra Pak*, [1996] ECR I-05951, para. 24.
[11] Opinion of Advocate General Fennelly in *Compagnie Maritime Belge and others v. Commission*, [2000] ECR I-1365, para. 137.
[12] Van Bael, Bellis J-F. (ed.), *Competition Law Of The European Community*, The Hague 2005, p. 119; E. Szyszczak, *Controlling Dominance in European Markets* [in:] *Fordham International Law Journal*, 2011/6(33), p. 1757.

4. Dominant Companies

Facebook, Google and Microsoft. These are the companies I am choosing as the brightest examples. Examples of abuses, dominance, strong position on several markets and finally because they are extremely well known names in the world. Simply, everyone knows them and something about their actions.

The first question is, are these companies really dominant, or can they be called super dominant? It is easy to make this kind of assumption, but equally easy is the realization that when it comes to legal definitions, nothing is that obvious.

Google and Microsoft have already been accused of abusing their dominant positions.[13] The European Commission stated that these companies are dominant on respective markets. Microsoft was even called super dominant on the market of operating systems.[14] Case closed, these companies are dominant.

What with Facebook, my third example? So far Facebook has never been an object of a competition law investigation, nor has it been accused of abusing its position. In my opinion, according to competition law, Facebook is not a dominant company on any specific market. Why? Because the dominance of the company is investigated only if the company is accused of conducting abuses. Could I then just say "case closed, Facebook is not dominant on any market"? No. The fact is that Facebook is dominant on the market of social media. To what extent, this is not exactly established.

The way and the moment competition law decides that a particular company is dominant, causes some problems and again forces me to avoid typical legal understanding of the term "dominance". In my dissertation I need to refer to Facebook as to the dominant company without using any additional qualification, such as "in fact" or "as the numbers indicate".

5. The New Dominance

I support the idea that when it comes to global dominant companies, or companies considered to be super dominant it is very rarely that they abuse the position they own. It could be said that they became victims of their success. Google and Microsoft are the brightest examples. In the case of Google this is a rather widely accepted opinion[15]. Microsoft is more

[13] Decision of European Commission from 24.03.2004 r. in T-201/04 case, *Microsoft*, point 18,
D. A. Crane, *Search Neutrality and Referral Dominance*, [in:] *Journal of Competition Law & Economics*, 8(3), p. 459, http://www.theregister.co.uk/2012/05/21/joaquin_almunia_google_statement/ (access June 2015).
[14] SPEECH/07/539, 17.09.2007 r., R. Whish, *Competition Law 6th Edition*, New York 2009, p. 185.
[15] S. van Loon, *Chapter 2. The Power of Google: First Mover Advantage or Abuse of a Dominant Position*, [in:], *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, A. Lopez-Tarruella (ed.), The Hague 2012, p. 10.

known for being just an abuser. I prefer to include Microsoft as victim, as a kind of "elephant in porcelain shop" – the company already that big and influential that it sometimes acts against competition law rules without really having an intention of doing so. The European Commission and The General Court would not agree with me, but this is my opinion which was a base for my master thesis "The Prohibition of Abuse of a Dominant Position in the Light of the *Microsoft* Case". In there I suggest that Microsoft was a subject of a long proceeding and was fined not because of intentional abuses, but because of its superdominant position, which was and is a danger to European companies which happen to be also Microsoft's competitors. I argue that Microsoft's behavior is not negatively influencing consumers and users.

On the other hand, what needs to be underlined, when it comes to abuses in the area of data protection and privacy, is that it does not matter why the company is dominant or whether it is a victim or an abuser. The situation is different. Abusing the dominant position, in competition law understanding, is about the market power and has an economic basis. The difference in US Antitrust Law and EU Competition Law shows us that it is not obvious what the reaction should be. Should we try to eliminate monopolies, but at the same time allow smaller companies to defend themselves and focus on protecting consumers (US Antitrust Law)[16], or should we protect consumers indirectly by protecting smaller companies (EU Competition Law)[17]? I don't think it is far from the truth to say that with widely understood data protection it is easier. It is about privacy and data that needs to be protected and it does not matter if the company is abusing its position on purpose, accidentally or as a victim of its extremely strong market position.

The problem of an insufficient definition of dominance, for the purpose of my dissertation, can to be partially solved by naming requirements for companies' dominance in the area of data protection and privacy. These requirements must be based on competition law as I do not want to isolate my work and ideas from the existing legal solutions and concepts.

In my dissertation, I would like to use companies' dominant position in very specific ways. The exact market share is not what I am interested in. Facebook is an example of very influential and powerful entity that doesn't have exact market shares, yet I do not think there are any doubts whatsoever that is has dominant position. Especially considering that there are ways to establish monopoly of Facebook on the Social Media market.[18]

[16] J. Majcher, *Dostęp do urządzeń kluczowych w świetle orzecznictwa antymonopolowego*, Warszawa 2005, p. 34.
[17] A. Jones, B. Sufrin, *EC Competition Law Third Edition*, New York 2008, p. 571.
[18] http://thenextweb.com/socialmedia/2012/06/10/facebook-is-eating-the-world-except-for-china-and-russia-world-map-of-social-networks/ (access June 2015).

Having that in mind I would like to propose the following requirements for deciding whether the company holds a dominant position or not, without starting an investigation under competition law:

- the company has to have global and multinational presence,
- strong overall market position,
- strong economic position,
- possible legal influence;

Of course the companies to meet my requirements and be useful in course of my work, must deal on the daily basis with large amount of data, possibly collected in connection with their profile.

As can be easily recognized these requirements have origins in competition law. This way it simplifies their application and the understanding.

a. Global and Multinational

What does it mean that the company must be global and multinational? The role of this requirement is to exclude all the entities which are considered to be dominant on the market of just one country or even just one continent. Therefore there is no place for Yandex[19] which is the biggest search engine on the Russian market[20] or Baidu[21], having the same position on the Chinese market.[22]

Global and multinational, these give me only companies having their presence and interests all over the world, reaching everyone, whether willingly or not. Some companies, may have headquarters in one, specific place, but in fact act like several smaller and often independent entities. For example, Facebook is after all everywhere, but this is an American company established under US law having its headquarter in United States. At the same time having a European headquarter in Ireland, in the European Union.[23]

[19] http://www.yandex.com/
[20] About 60% of Russian market: http://marketrealist.com/2014/03/yandex-market-share-increase-powered-search/, http://connect.icrossing.co.uk/a-closer-look-at-yandexs-market-share-in-russia_12575 (access June 2015).
[21] http://www.baidu.com/
[22] About 70% of Chinese market: http://www.chinainternetwatch.com/category/search-engine/ (access June 2015).
[23] *Facebook's new headquarters is located at 1 Hacker Way*, http://www.zdnet.com/article/facebooks-new-headquarters-is-located-at-1-hacker-way/ (access June 2015).

b. Strong Overall Market Position

The custom in competition law decides when the company holds a dominant position and on what market etc. As I have written already, Facebook, for example, has a very specific situation in which assessing by numbers its position is rather difficult. Microsoft is, according to the competition law, definitely not a dominant company on the search engine market. Google on the other hand holds strong position on all markets they are involved.

"Strong Overall Market Position" requires something different. For a company to be considered as dominant for my purposes, in the area of data protection and privacy, it must hold a position that allows it to collect and process large amounts of data. Microsoft may not be the owner of the most popular search engine (Bing) but together with all the Windows operating systems (including PC and mobile solutions), Skype, Internet Explorer, Xbox Live and Windows Live, it has access to one of the biggest databases in the world. Almost the same applies to Google. Facebook gained access to one of the biggest databases in a different way, but result is the same.

Microsoft, Google, Facebook - similar and different at the same time, found their ways to collect incredibly large amount of data. How many more companies in the world can say that they have access to information about people from every corner of the world?

c. Strong Economic Position

Strong economic position in this case means that the selected companies are able to pay any given financial fines put on them without actually feeling this.

Microsoft is a great example. Losing the *Microsoft* case cost the company together around 1.2 billion euro.[24] It is still the highest fine ever paid in the history of European Union. The European Commission called it a huge success.

But was it a big loss for Microsoft? Microsoft is the first company to be a subject to such a high penalty. This is a record, but keep in mind that, for example, Microsoft's revenue in 2005 was 39.78 billion and net profit 12.25 billion. The fine of 1.2 billion is the sum of all fines that Microsoft had to pay during the 10 years of the process against the European Commission. It is not hard to imagine that in this perspective 1.2 billion euro no longer looks that big.[25]

[24] Microsoft underwent a series of investigations and settlements, racking up a total of more $3 billion in European fines over the course of a decade, including a penalty in 2013 for failing to adhere to an earlier settlement.
[25] D. Poeter, *EU Slams Microsoft With Record $1.35 Billion Fine*, http://www.crn.com/news/applications-os/206900563/eu-slams-microsoft-with-record-1-35-billion-fine.htm, A. Słojewska, *Bruksela nie kończy walki z Microsoftem*, "Rzeczpospolita", 13.07.2006.

Strong economic position means that a company does not have to fear any possible fine that can be given under existing laws. That the fine may just become the cost of running the company. Of course I assume that there is a number, a fine high enough to scare even one of these companies. The European Parliament, for instance, has called for a breakup of Google.[26] A breakup will almost certainly not happen, but for Google, its inability to reach a settlement with the European Commission despite years of trying means the company could still potentially face a fine of nearly $6 billion, or 10 percent of global annual sales, and restrictions on its freedom to do business in Europe if it is eventually found to have broken EU competition laws.[27]

d. Possible Legal Influence

During the KnowRight 2012 conference in Helsinki, the Finnish Data Ombudsman Rejio Aarnio spoke about 25 years of Data Protection in Finland and asked the question, "Are we ready?" He listed a number of solutions which are planned to be implemented into European Union law. Most of these solutions already exist in Finnish law. Regardless of that, even Finland is having troubles dealing with Facebook.[28]

Actions of companies I am interested in, may result in law becoming outdated or at least insufficient long before it is even enacted. It may be one of the biggest issues for the new data protection regulation.

There is also possible way of influencing law. Every time Google or Facebook works on a revised version of, for example, their Privacy Policies they may present innovative ideas and solutions.[29]

6. Summary

Competition law does not define the term "dominance" in legislation. Dominance, in a rather unclear fashion, was explained in EU case law, leaving a lot to discuss. Being not really defined, dominance on the other hand is in competition law quite specific and leaves usually

---

[26] *The Misbegotten 'Right to Be Forgotten'*, http://www.usnews.com/debate-club/should-there-be-a-right-to-be-forgotten-on-the-internet/the-misbegotten-right-to-be-forgotten (access June 2015).
[27] *E.U. Parliament Passes Measure to Break Up Google in Symbolic Vote*, http://www.nytimes.com/2014/11/28/business/international/google-european-union.html?_r=0 (access June 2015).
[28] C. Maurieni, *Facebook is Deception (Volume One)*, 2012, http://books.google.fi/books?id=s6TxlJ1v5y4C&printsec=frontcover&dq=Facebook+is+Deception+(Volume+One)&hl=pl&sa=X&ei=7GMKUZDyGInitQaez4DYAQ&ved=0CCwQ6AEwAA (access June 2015).
[29] R. Rodrigues, *Privacy on Social Networks: Norms, Markets, and Natural Monopoly* [in:] *The Offensive Internet*, S. Levmore, M.C. Nussbaum (ed.), Cambridge, Massachusetts, London 2010, p. 241-250.

no doubt which company is dominant and on what market. Yet, it causes some uncertainties in some cases. Specifically, when I want to talk about dominant companies in the area of data protection and privacy. Saying only that selected companies hold given numbers on some markets, or that they are not dominant only in very few places in the world is not enough.

When it comes to processing data and dealing with privacy issues, there are several companies which are different compared to others. They are everywhere, but at the same time nowhere. They hold a strong position on many markets, together having the possibility to create enormous data bases. They conduct or are able to conduct abuses in connection with the data they process. Existing law is insufficient to stop them. Finally, unlike in competition law there is as of yet no way of cooperating with the abuser.

It is all fine, but why in fact do I believe we need a different dominance? Marking a company as a monopolist, dominant or super dominant means that the company has special responsibilities. Mainly because the special position may cause more harm. It is more or less the victim of the size or position. Using competition law requirements to asses if a company is in a dominant position is not enough. Microsoft does not have a monopoly on any market that alone could cause danger to privacy or data protection. Facebook is not even a monopolist, at least officially, although it is treated as such by europe-v-facebook.org.[30] Finally Google is an exception, but this exception shows how strong, on the single product market the company has to be, to be seen and recognized as a threat.

Seeing a company as a subject on multiple markets, not always connected with each other, by any means, may help in recognizing the problem earlier. If in competition law a recognized monopolist is treated as a potential abuser, in the area of data protection and privacy we should look for companies being able to collect data without any limitation thanks to the position they hold on several markets. Competition law is focused on economy, my point of view is focused on privacy and security. In both cases we cannot stop the companies from being dominant, but we can start asking questions about necessity of their actions. And if we recognize them early enough as potential abusers, we may have more chances to avoid situation similar to the one with Facebook, Google and Microsoft.

For discussion is whether we should treat these companies aggressively, or simply look for a compromise. Although it seems that recently European Parliament decided to take aggressive approach. And not only European Parliament. Also EU states, as well as citizens. We have example of Max Schrems, an Austrian student who along with 25,000 fellow plaintiffs, has

[30] *Open Social Networks*, http://www.europe-v-facebook.org/EN/Objectives/objectives.html (access June 2015).

sued Facebook for privacy breaches.[31] Belgium's Commission for the Protection of Privacy is launching a legal case, alleging that Facebook is not complying with local privacy legislation.[32] Hopefully soon we will see where does it lead and what practical consequences it will bring to data protection and to dominant companies' behavior.

[31] Austrian student's lawsuit vs Facebook bogged down in procedure, http://www.reuters.com/article/2015/04/09/us-facebook-austria-lawsuit-idUSKBN0N019420150409 (access June 2015).
[32] Privacy Commission takes Facebook to court, http://deredactie.be/cm/vrtnieuws.english/News/1.2367528?devicetype=mobile (access June 2015).

Bibliography

1. Anawalt H.C., *International Intellectual Property, Progress, and the Rule of Law*, "Santa Clara Computer and High Technology Law Journal" 2003/19.
2. Arnold R., *Website-blocking injunctions: the question of legislative basis*, „European Intellectual Property Review" 2015/10.
3. Ashley K., *Toward Extracting Information from Public Health Statutes using Text Classification and Machine Learning, Legal Knowledge and Information Systems*, Jurix 2011.
4. Balazs B., *Coda: A Short History of Book Piracy* [in:] *Media Piracy in Emerging Economies*, J. Karaganis (ed.) Social Science Research Council 2011.
5. Baldwin C.Y., Hippell E., *Modeling a Paradigm Shift: From Producer Innovation to User and Open Collaborative Innovation*, "Harward Buisness School Working Paper", http://ssrn.com/abstract=1502864 or http://dx.doi.org/10.2139/ssrn.1502864 (access 18.04.2013).
6. Ballardini R.M., *Scope of IP Protection for the Functional Elements of Software* [in:] *In Search of New IP Regimes*, N. Bruun (ed.), Helsinki 2010.
7. Bangemann M., *A new World Order for Global Telecommunications – The Need for an International Charter*, http://www.ispo.cec/be/infosoc/promo/speech/geneva.html.
8. Bankowski Z., Del Mar M. (eds.), *Moral Imagination and the Legal Life: Beyond Text in Legal Education*, Farnham/Burlington 2013.
9. Bankowski Z., Mungham G., *Images of law*, London 1976.
10. Benkler Y., *The Wealth of Networks: How Social Production Transforms Markets and Freedom*, Yale 2006, http://www.benkler.org/Benkler_Wealth_Of_Networks.pdf (access 17.02.2014).
11. Berman D., *Toward a New Format for Canadian Legislation. White paper* 2000.
12. Biddle P., England P., Peinado M., Willman B., *The Darknet and the Future of Content Distribution* [in:] *Digital Rights Management*, J. Feigenbaum (ed.), Berlin/Heidelberg 2003.
13. Bonina C., *New business models and the value of open data: definitions, challenges and opportunities*, http://www.nemode.ac.uk/wp-content/uploads/2013/11/Bonina-Opendata-Report-FINAL.pdf;
14. Bounie D., Waelbroeck P., Bourreau M., *Piracy and the Demand for Films: Analysis of*

Piracy Behavior in French Universities, "Review of Economic Research on Copyright Issues" 2006/2, http://ssrn.com/abstract=1144313, (access 13.10.2014).

15. Breitschaft A., *Evaluating the linear/non-linear divide - are there any better factors for the future regulation of audiovisual media content? "*Entertainment Law Review" 2009/8.
16. Brin D., *The Transparent Society*, New York 1997.
17. Brodecki Z., *Epilog. Technologie i prawo w społeczeństwie wiedzy* [in:] *Świątynia w cyberkulturze. Technologie cyfrowe i prawo w społeczeństwie wiedzy*, A.M. Nawrot, Z. Brodecki, Gdańsk 2007.
18. Brodowski D., Freiling F.C., *Cyberkriminalität, Computerstrafrecht und die digitale Schattenwirtschaft*, Berlin 2011.
19. Brown C.L.T., *Computer Evidence: Collection and Preservation*, Boston 2009.
20. Brunschwig C., *Visualisierung von Rechtsnormen, Legal Design*, Zürich 2001.
21. Brustein J., *The Companies' Lines on Prism*, June 07, 2013, http://www.businessweek.com/articles/2013-06-07/the-companies-lines-on-prism
22. Bygrave L., *Data Privacy Law. An International Perspective*, Oxford 2014.
23. Cameron J., *[Opinion] Approaches to the Problems of Multimedia,* "European Intellectual Property Review" 1996/3.
24. Campbell-Kelly M., Valduriez P., *A Technical Critique of Fifty Software Patents*, "Marquette Intellectual Property Law Review" 2005/2.
25. Carnap R., Bar-Hillel Y., *An outline of the theory of Semantic information*. Research Laboratory of Electronic, Massachusetts Institute of Technology, Report No. 247, 1952
26. Casey E., *Digital Evidence and Computer Crime*, Waltham 2011.
27. Casey E., *Reconstructing Digital Evidence* [in:] *Crime Reconstruction*, W.J. Chisum, B.E. Turvey, Burlington 2006.
28. Castendyk O., Dommering E., Scheuer A., *European Media Law.* Alphen a/d Rijn 2008.
29. Cattaneo G., Kolding M., Bradshaw D., Folco G., IDC, *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up*, SMART 2011/0045, D2-Interim Report, 24 February 2012 http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf.
30. Clough J., *Principles of Cybercrime*, Cambridge 2010.
31. Cook T., *EU Intellectual Property Law*, Oxford 2010.
32. Cooter R., Ulen T., *Introduction to Law and Economics*, 2007,

http://works.bepress.com/robert_cooter/56.

33. Cornes R., Sandler T., *The theory of externalities, public goods and club goods*, Cambridge 2003.
34. Crane D.A., *Search Neutrality and Referral Dominance*, "Journal of Competition Law & Economics" 2012/3, http://www.theregister.co.uk/2012/05/21/joaquin_almunia_google_statement/
35. Dejean S., *What can we learn from empirical studies about piracy?*, "CESifo Economic Studies, Oxford University Press (OUP): Policy E - Oxford Open Option D" 2009/2, https://hal.inria.fr/file/index/docid/963851/filename/1draft.pdf (access 12.12.2014).
36. Dejean S., *What can we learn from empirical studies about piracy?* "CESifo Economic Studies" 2009/2.
37. Diamond E., Bates S., *Law and order comes to cyberspace*, "MIT Technology Review" 1995/98.
38. Dority B., *Ratings and the V-chip,* "The Humanist" May/June 1997.
39. Egitto L., *Certifying Uncertainty: Assessing the Proposed Directive on the Patentability of Computer Implemented Inventions*, "The Journal of Information, Law and Technology" 2004/3 http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/egitto/ (access 12.1.2015).
40. Endeshaw A., *Reconfiguring Intellectual Property for the Information Age: Towards Information Property?*, "The Journal of World Intellectual Property" 2004/3.
41. Esayas S.Y., *A walk in to the cloud and cloudy it remains: The challenges and prospects of 'processing' and 'transferring' personal data*, "Computer Law and Security Review" 2012/6.
42. Esteve A., *Patent Protection of Computer-Implemented Inventions Vis-À-Vis Open Source Software*, "The Journal of World Intellectual Property" 2006/3.
43. Favalle M., Kretschmer M. and Torremans P. C., *Is there a EU Copyright Jurisprudence. An empirical analysis of the workings of the European Court of Justice*, available at Social Science Research Network, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2643699 (access 4.10.2015)
44. Feigenson N., *The Visual in Law: Some Problems for Legal Theory in Law*, "Culture and the Humanities" 2014/1.
45. Garofalo R., *From Music Publishing to MP3: Music and Industry in the Twentieth Century*, American Music 1999/3.
46. Geiger C., *"Constitutionalizing" Intellectual Property Law? The Influence of*

Fundamental Rights on Itellectual Property in the European Union? "International Review of Intellectual Property and Competition Law" 2006/37.

47. Gentile A., Anderson C.A., *Violent Video Games: Effects on Youth and Public Policy Implications* [in:] *Handbook of Children, Culture, and Violence*, N.E. Dowd, D.G. Singer, R.F. Wilson (eds.), 2006.
48. Gęsicka D.K., *Nakazy sądowe kierowane do pośredników w komunikacji elektronicznej*, Kwartalnik Prawa Prywatnego 2015/2.
49. Gęsicka D.K., *Wyłączenie odpowiedzialności dostawców usług sieciowych za treści użytkowników*, Warszawa 2014.
50. Girardi D., Palmirani M., *Legal Issues and Economic Exploitation of Open Government Data*, "Jusletter IT"15 May 2013.
51. Giurgiu A., Metzdorf J., *Smart TV – Smarte Regulierung?* [in:] *Big Data & Co., Neue Herausforderungen für das Informationsrecht*, J., Taeger (ed.), Oldenburg, Germany 2014.
52. Gleeson N., Walden I., *It's a jungle out there'?: Cloud computing, standards and the law*, "European Journal of Law and Technology" 2014/2.
53. Gliściński K., *Rola modelu ochrony dóbr niematerialnych w ramach Społecznego Systemu Wspierania Innowacji — zarys analizy*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego Prace z Prawa Własności Intelektualnej" 2013/3.
54. Gołaczyński J. (ed.), *Ustawa o świadczeniu usług drogą elektroniczną.* Komentarz, Warszawa 2009.
55. Grabmair M., Ashley K.D., Hwa R., Sweeney P.M., *Toward Extracting Information from Public Health Statutes using Text Classification and Machine Learning* [in:] *Legal Knowledge and Information Systems. JURIX 2011: The Twenty-Fourth Annual Conference*, Atkinson K.M. (ed.), Amsterdam 2011.
56. Gratton E., *Should Patent Protection Be Considered for Computer Software-Related Innovations?*, "Computer Law Review & Technology Journal" 2003/7.
57. Guillou C.M., *The Reverse Engineering of Computer Software in Europe and the United States: A Comparative Approach*, "Columbia – VLA Journal of Law & the Arts" 1998/22.
58. Hanneman H.W.A.M., *The Patentability of Computer Software*, Boston 1985.
59. Harju V. (ed.), *Oikeuden näyttämöt. Kuvallisuus lainkäytössä*, Helsinki 2013.
60. Hellemans L., *Report on legal aspects of Cloud Services in the European public sector and legal project support (D2.1. Legal implications on cloud computing)*, Cloud for

Europe
1.5.2014http://www.cloudforeurope.eu/documents/10179/15444/D2.1+Legal+implications+on+cloud+computing+v1/023da045-4c78-4cd7-afe6-0a5de01c0347.

61. Hume G., LeRose B., Lloyd P., Kuiack S., *Report of the Cloud Computing Working Group*, *Appendix 1 – Due Diligence Guidelines*, Law Society of British Columbia, 27.01.2012.
62. Husovec M., *Injunctions against Innocent Third Parties: The Case of Website Blocking*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2013/4.
63. Huygen A., Helberger N., Poort J., Rutten P., Eijk N. van, *Ups and Downs; Economic and Cultural Effects of File Sharing on Music, Film and Games* (February 18, 2009) "TNO Information and Communication Technology Series", http://ssrn.com/abstract=1350451 or http://dx.doi.org/10.2139/ssrn.1350451 (access 10.09.2014).
64. Ignatin G.R., *Let the Hackers Hack: Allowing the Reverse Engineering of Copyrighted Computer Programs to Achieve Compatibility*, "University of Pennsylvania Law Review" 1992/5.
65. Jakubowicz K., *Media and democracy* [in:] *Media and Democracy*, Strasbourg, Council of Europe Publication 1998.
66. Johns A., *Piracy. The intellectual property wars from Gutenberg to Gates*, Chicago-London, 2009.
67. Jones A., Sufrin B., *EC Competition Law Third Edition*, New York 2008.
68. Kachur R.L., Kleinsmith W.J., *The Evolution to the Cloud – Are Process Theory Approaches for ERP Implementation Lifecycles Still Valid?*, "Business Systems Review" 2013/3.
69. Kaczmarek P., *Tożsamość prawnika jako wykonawcy roli zawodowej*, Warszawa 2014.
70. Karaganis J., *Rethinking piracy* [in] *Media piracy in emerging economies*, J. Karaganis (ed.), Social Science Research Council 2011, http://www.scribd.com/doc/50196972/MPEE-1-0-1 (access 01.05.2012).
71. Karaganis J., *Social Science Research Council*, 2011, http://www.scribd.com/doc/50196972/MPEE-1-0-1 (access 01.05.2012).
72. Katsh A.M.E., *Law in a Digital World*, Oxford 1995
73. Kerr O.S, *Applying the Fourth Amendment to the Internet: A General Approach*, "Stanford Law Review" 2010/4.

74. Kerr O.S., *Searches and Seizures in a Digital World*, "Harvard Law Review" 2005/2.
75. Kerr O.S., *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, "Michigan Law Review" 2004/5.
76. Klafkowska-Waśniowska K., *Commentary to art. 18* [in:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, M. Namysłowska, D. Lubasz (eds.), Warszawa 2011.
77. Klafkowska-Waśniowska K., *Nowe formy audiowizualnych usług medialnych a przesłanka "odpowiedzialności redakcyjnej" w dyrektywie o audiowizualnych usługach medialnych. "*ZNUJ" 2014/2.
78. Kołakowski L., *O co nas pytają wielcy filozofowie. Trzy serie*, Kraków 2008.
79. Kołakowski L., *Ułamki filozofii*, Warszawa 2008.
80. Konopacka M., *Res privata* [in:] *Komparatystyka kultur prawnych*, Z. Brodecki, M. Konopacka, A. Brodecka-Chamera, Warszawa 2010.
81. Kopff A., *Wpływ postępu technicznego na prawa autorskie*, "Zeszyty Naukowe Uniwersytetu Jagiellońskiego, Prace z Prawa Własności Intelektualnej" 1988/48.
82. Kretschmer M., Private Copying and Fair Compensation: An empirical study of copyright levies in Europe, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/310183/ipresearch-faircomp-201110.pdf (access 18.2.2015).
83. Kuan Hon W., Hörnle J., Millard Ch., *Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? The Cloud of Unknowing*, "International Review of Law, Computers & Technology" 2012/2-3.
84. Kulk S., Borgesius F., *Filtering for Copyright Enforcement in Europe after the SABAM cases*, "European Intellectual Property Review" 2012/11.
85. Li X., *Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society*, Turku 2008.
86. Litwiński P., *Anonimowość w sieci. Zagadnienia udostępniania danych osobowych* [in:] *Internet. Prawo-informatyczne problemy sieci, portali i e-usług*, G. Szpor, W. Wiewiórowski (eds.), Warszawa 2012.
87. Łojko E., *Role i zadania prawników w zmieniającym się społeczeństwie. Raport z badań*, Warszawa 2005.
88. Luettgen D.G., *Functional Usefulness vs. Communicative Usefulness: Thin Copyright Protection for the Nonliteral Elements of Computer Programs*, "Texas Intellectual

Property Law Journal" 1996/4.

89. Lutz H, *The distinction between linear and non-linear services in the new proposal of the audiovisual media directive*, "Computer and Telecommunications Law Review" 2006/12.
90. Magalhaes G., Roseira C., Manley L., *Business models for open government data*, opendata500.thegovlab.org/files/Business_Models_for_OGD.pdf.
91. Mahler T., *A Graphical User-Interface for Legal Texts?* [in:] *Internationalisation of Law in the Digital Information Society: Nordic Yearbook of Law and Informatics*, D.J.B. Svantesson, S. Greenstein (eds.), 2010–2012.
92. Mahler T., *A Graphical User-Interface for Legal Texts?* [in:] *Internationalisation of Law in the Digital Information Society. Nordic Yearbook of Law and Informatics 2010–2012*, Svantesson D.J.B., Greenstein S. (eds.), Copenhagen 2013.
93. Majcher J., *Dostęp do urządzeń kluczowych w świetle orzecznictwa antymonopolowego*, Warszawa 2005.
94. Mason S., *Encrypted data* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012.
95. Mason S., *Introduction* [in:] *International Electronic Evidence*, S. Mason (ed.), London 2008.
96. Mason S., Sheldon A., *Proof: the investigation, collection and examination of digital evidence* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012.
97. Mattila H.E.S., *From Judge's Robes to Banyan Leaves. The Visual Symbols of Justice in Historical and International Perspective* [in:] *Oikeuskieli ja säädöstieto. Suomenkielinen lakikirja 250 vuotta*, Mattila H.E.S., Piehl A., Pajula S. (eds.), Helsinki 2010.
98. Maurieni C., *Facebook is Deception (Volume One)*, 2012, http://books.google.fi/books?id=s6TxlJ1v5y4C&printsec=frontcover&dq=Facebook+is+Deception+(Volume+One)&hl=pl&sa=X&ei=7GMKUZDyGInitQaez4DYAQ&ved=0CCwQ6AEwAA
99. May Ch., Sell S.K., *Intellectual property rights. A critical history*, London 2006.
100. Mell P., Grance T., *The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology*, National Institute of Standards and Technology Gaithersburg, September 2011.
101. Metzdorf J., *The Implementation of Audiovisual Media Services Directive by National Regulatory Authorities. National Responses to Regulatory Challenges.* JIPITEC 2014/2.
102. Modéer K.-Å., Optimal Legal Cultures, Globalization and Modernities 1999.

103. Modéer K.-Å., *Optimal Legal Cultures? Modernity and Continuity in National and Global Legal Cultures* [in:] *Globalizations and Modernities – Experiences and Perspectives of Europe and Latin America*, G. Therborn (ed.), Stockholm 1999.
104. Modéer K.-Å., *Optimala rättsliga kulturer?*, "Juridisk Tidsskrift" 1999–2000/1.
105. Nagel D., *Network Blocking in the EU: A Slippery Slope to (Third Party) Censorship? How the CJEU Missed to Give a Crucial Guidance in his Judgement on UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH, C-314/12, Decision 27 March 2014*, „Computer Law Review International" 2014/4.
106. Namysłowska M., Lubasz D. (eds.), *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustaw*, Warszawa 2011.
107. Niiniluoto Il., *Informaatio, Tieto ja Yhteiskunta (Information, Knowledge, and Society)*, Helsinki 1989.
108. Oberholzer-Gee F., Strumpf K., *The Effect of File Sharing on Record Sales: An Empirical Analysis*, "Journal of Political Economy" 2007/1.
109. Ożegalska-Trybalska J., *Ochrona programów komputerowych i wynalazków implementowanych za pomocą komputera* [in:] *Komputer – Człowiek – Prawo*, W. Lubaszewski (ed.), Kraków 2007.
110. Palmirani M., Mockus M., *Open Government Data Licensing Framework* [in:] *Electronic Government and the Information Systems Perspective Fourth International Conference,* A. Kő, E. Francesconi (eds.), EGOVIS 2014, Valencia, Spain, September 1-4, 2015.
111. Patterson L.R., *Copyright in Historic Perspective*, Vanderbilt University 1968.
112. Perchaud S., *Software Patents and Innovation*, "Journal of Information, Law & Technology" 2003/1, http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2003_1/perchaud/ (access 12.01.2015).
113. Pérez-Cota M., Gonçalves R., Moreira F., *Cloud Computing Decisions in Real Enterprises*, [in:] *Agile Estimation Techniques and Innovative Approaches to Software Process Improvement* R. Colomo-Palacios (ed.), IGI Global 2014.
114. Peukert Ch., Claussen J., Kretschmer T., *Piracy and Movie Revenues: Evidence from Megaupload: A Tale of the Long Tail?*, http://ssrn.com/abstract=2176246 or http://dx.doi.org/10.2139/ssrn.2176246 (access 12.09.2014).
115. Philips J.C., *Sui Generis Intellectual Property Protection for Computer Software*, "The George Washington Law Review" 1992/60.
116. Pihlajamäki A., *Tietojenkäsittelyrauhan rikosoikeudellinen suoja*, *Datarikoksia koskeva*

sääntely Suomen rikoslaissa, Helsinki 2004.

117. Poeter D., *EU Slams Microsoft With Record $1.35 Billion Fine*, http://www.crn.com/news/applications-os/206900563/eu-slams-microsoft-with-record-1-35-billion-fine.htm,
118. Polański P., *Odpowiedzialność prawna za treści rozpowszechniane w Internecie/Legal liability for content disseminated over the Internet*, Warszawa 2012, http://www.natolin.edu.pl/pdf/zeszyty/Natolin_Zeszty_48.pdf (access February 2015).
119. Polański P., *Prawo Internetu*, Warszawa 2014.
120. RCMP, *Cybercrime: An Overview of Issues and Incidents in Canada*, 2014.
121. *Ridgeway S., The Audiovisual Media Services Directive - what does it mean, is it necessary and what are the challenges to its implementation?, "*Computer and Telecommunications Law Review" 2008/4.
122. Rigaux F., *La protection de la vie privée et des autres biens de la personnalité*, Brussels 1990.
123. Rob R., Waldfogel J., *Piracy on the High C's: Music Downloading, Sales Displacement, and Social Welfare in a Sample of College, Students*, National bureau of economic research 2004, Working Paper 10874 http://www.nber.org/papers/w10874 (access 14.03.2015).
124. Rodrigues R., *Privacy on Social Networks: Norms, Markets, and Natural Monopoly*, [in:] *The Offensive Internet*, S. Levmore, M.C. Nussbaum (ed.), Cambridge, Massachusetts, London 2010.
125. Saarenpää A., Lakikirjasta tietovarantoihin s. 289-310 in Mattila – Piehl – Pajula Oikeuskieli ja säädöstieto : suomenkielinen lakikirja 250 vuotta = Rättsspråk och författningsinformation : den finskspråkiga lagboken 250 (2010)
126. Saarenpää A., *Oikeusinformatiikka in Oikeusjärjestys* (2012)
127. Saarenpää A., *Lakikirjasta tietovarantoihin* [in:] *Oikeuskieli ja säädöstieto. Suomenkielinen lakikirja 250 vuotta*, H.E.S. Mattila, A. Piehl, S. Pajula (eds.), Helsinki 2010.
128. Saarenpää A., *Oikeusinformatiikka* [in:] *Oikeusjärjestys. Osa I*, T. Tammilehto (ed.), Rovaniemi 2012.
129. Saarenpää A., *The Network society and legal information. Some observations from the Nordic point of view*, Law via the Internet 2011 conference paper, 2011.
130. Saarenpää A., *Towards legal information and legal knowledge. Some basic issues in Finnish perspective* [in:] *Festskrift till Peter Seipel*, Magnusson Sjöberg C., Wahlgren

P. (eds.), Stockholm 2006.
131. Samani R., Honan B., Reavis J., *CSA Guide to Cloud Computing. Implementing cloud privacy and security*, Syngress 2015.
132. Sandgren C., *Vad gör juristen? Och hur?*, "Juridisk Tidskrift" 1999–2000/3.
133. Sandgren, *Claes Vad gör juristen och hur?*, JT1999-2000.
134. Saunders D., *Authorship and copyright*, London 1992.
135. Sauter W., *EU Regulations for the Convergence of Media, Telecommunications, and Information Technology: Arguments from Constitutional Approach?* Zentrum für Europäische Rechtspolitik an der Universität Bremen Diskussionpapier 98/1.
136. Savin A., *EU Internet Law*, Cheltenham, Northampton 2013.
137. Savona E.U., Mignone M., *The Fox and the Hunters: How IC Technologies Change the Crime Race* [in:] *Crime and Technology: New Frontiers for Regulations, Law Enforcement and Research,* E. Savona (ed.), Dordrecht 2004.
138. Schafer B., Mason S., *The characteristics of electronic evidence in digital format* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012.
139. Scharf A., *The Media and the European Model of Society*, European Audiovisual Conference Birmingham, 6-8 April 1998.
140. Scheuer A., *Convergent Devices, Platforms, and Services for Audiovisual Media. Challenges set by Connected TV for the EU Legislative Framework*, IRIS Plus 3/2013.
141. Sevola P*., Proportionality of Website Blocking: Internet Connectivity Providers as Copyright Enforcers*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2014/5.
142. Sibiga G. (ed.), *Główne problemy prawa do informacji*. Warszawa 2013.
143. Sieber U., *Legal Aspects of Computer-Related Crime in the Information Society*, 1998.
144. Sieber U., *Straftaten und Strafverfolgung im Internet*, München 2012.
145. Słojewska A., *Bruksela nie kończy walki z Microsoftem*, "Rzeczpospolita", 13.07.2006.
146. Smith G., *Internet law and regulation,* London 1996.
147. Smith M.D., Telang R., *Assessing the academic literature regarding the impact of media piracy on sales*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2132153 (access 12.12.2014).
148. Solove D.J, *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven 2011.
149. Spoenle J., *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?*, Strasbourg 2010.

150. Stiglitz J.E., *Economic foundations of intellectual property law*, "Duke Law Journal" 2008/57.
151. Stiglitz J.E., *The price of inequality,* London 2012.
152. Sunde I.M., *IKT-kriminalitet: etterforskningsmetoder og personvern*, "Nordisk Tidsskrift for Kriminalvidenskab" 2000/3.
153. Susskind R., *Koniec świata prawników? Współczesny charakter usług prawniczych*, Warszawa 2010.
154. Susskind R., *Prawnicy przyszłości*, Warszawa 2013.
155. Sylvester C., *Anatomy of a Footnote*, "Security Dialogue" 2007/4.
156. Szpor G., Wiewiórowski W. (eds.), *Internet. Prawo-informatyczne problemy sieci, portali i e-usług*, Warszawa 2012.
157. Sztobryn K., *Ochrona programów komputerowych w prawie własności intelektualnej Unii Europejskiej*, Warszawa 2015.
158. Szyszczak E., *Controlling Dominance in European Markets*, "Fordham International Law Journal" 2011/6.
159. Tatarkiewicz W., *Historia filozofii*. Warszawa 1958.
160. Twardowski K., *O filozofii średniowiecznej wykładów sześć*, Warszawa 1910.
161. UNODC, *Comprehensive Study on Cybercrime*, New York 2013.
162. Van Alsenoy B., *Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in Directive 95/46/EC*, "Computer Law and Security Review" 2012/1.
163. Van Bael, Bellis J-F. (ed.), *Competition Law Of The European Community*, The Hague 2005.
164. Van Eecke P., *Cloud Computing. Legal issues*, http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf.
165. Van Loon S., *The Power of Google: First Mover Advantage or Abuse of a Dominant Position*, [in:] *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models,* A. Lopez-Tarruella (ed.), The Hague 2012.
166. Vaver D. (ed.), *Intellectual Property Rights Critical Concepts in Law*, Oxford 2006.
167. Vaver D., *Invention in Patent Law: A Review and a Modest Proposal*, "International Journal of Law and Information Technology" 2003/11.
168. Vickery G., *Review of recent studies on PSI re-use and related market developments*, August 2011.

169. Vitorino A., Recommendations resulting from the mediation on private copying and reprography levies, Brussels, 31.1.2013, http://ec.europa.eu/internal_market/copyright/docs/levy_reform/130131_levies-vitorino-recommendations_en.pdf (access 18.2.2015).
170. Vitorino A., Statement at the occasion of the Conference: *"The Internet and the Changing Face of Hate"*, Berlin, 26.06.2000, http://www.europa.eu.int/rapid/start/cgi
171. Voyatzis P., Burkhard S., *The Battle of the Precendents: Reforming Legal Education in Mexico Using Computer-Assisted Visualization* [in:] *Moral Imagination and the Legal Life,* Z. Bankowski, P. Maharg, M. Del Mar (eds.), Ashgate Publishing Ltd. 2013.
172. Voyatzis P., Schafer B., *The Battle of the Precedents: Reforming Legal Education in Mexico Using Computer-Assisted Visualization* [in:] *The Moral Imagination and the Legal Life: Beyond Text in Legal Education*, Bankowski Z., Del Mar M. (eds.), Farnham/Burlington 2013.
173. Waldfogel J., *Music File Sharing and Sales Displacement in the iTunes Era*, "Information Economics and Policy" 2010/22.
174. Wang F. F., *Jurisdiction and Cloud Computing: Further Challenges to Internet Jurisdiction*, "European Business Law Review" 2013/5.
175. Weir G.R.S, Mason S., *The sources of digital evidence* [in:] *Electronic Evidence*, S. Mason (ed.), London 2012.
176. Whish R., *Competition Law 6th Edition*, New York 2009.
177. Whitmore A., Agarwal A., Da Xu L., *The Internet of Things—A survey of topics and trends*, Springer 2014.
178. Wiewiórowski W., *Ponowne przetwarzanie informacji publicznej zawierającej dane osobowe* [in:] *Główne problemy prawa do informacji*, G. Sibiga (ed.), Warszawa 2013.
179. Wiggins E.C., *What We Know and What We Need to Know About the Effects of Courtroom Technology*, "William & Mary Bill of Rights Journal" 2004/3.
180. Wikström K., *Kuka tarvitsee oikeuslähdeoppia* [in:] *Oikeus – kulttuuria ja teoriaa. Juhlakirja Hannu Tolonen*, Tala J., Wikström K. (eds.), Turku 2005
181. Wiśniewski A., *Znaczenie wolności słowa w państwie demokratycznym*, "Gdańskie Studia Prawnicze" 2000/7.
182. Wood J., *The Darknet: A Digital Copyright Revolution*, "Richmond Journal of Law and Technology" 2010/4.
183. Wróbel I., *Odpowiedzialność dostawcy dostępu do Internetu jako pośrednika, którego usługi są wykorzystywane w celu naruszenia praw autorskich lub pokrewnych – glosa*

do wyroku Trybunału Sprawiedliwości z 27.03.2014 r. w sprawie C-314/12, UPC Telekabel Wien GmbH przeciwko Constantine Film Verleih GmbH i Wega Filmproduktionsgesellschaft GmbH, „Europejski Przegląd Sądowy" 2015/4.

184. Zalewski K., Celmer S., Firlej J., Murawska-Najmiec E., Woźniak A., *Telewizja hybrydowa: szanse, zagrożenia i wyzwania regulacyjne*. KRRiT, Warsaw, May 2013, http://www.krrit.gov.pl/Data/Files/_public/Portals/0/publikacje/analizy/tv-hybrydowa_raport_2013-05-16_2_def-2.pdf.
185. Zentner A., *Measuring the Effect of File Sharing on Music Purchases*, "J. Law and Econ." 49 (April): 63–90. 2006.
186. Zingales N., *Virtues and Perils of Anonymity. Should Intermediaries Bear the Burden?*, "Journal of Intellectual Property, Information Technology and Electronic Commerce Law" 2014/5.
187. Zirk-Sadowski M., *Uczestniczenie prawników w kulturze*, „Państwo i Prawo" 2002/9.
188. Zittrain J., The Generative Internet, "Harvard Law Review" 2006/7.