

KnowRight 2012

Interaction of Knowledge Rights, Data
Protection and Communication

25 Years of Data Protection in Finland

OCG Forum Privacy 2013



books@ocg.at
BAND 299

Sämtliche in diesem Buch verwendeten personenbezogenen Bezeichnungen sind geschlechtsneutral zu verstehen. Zwecks besserer Lesbarkeit wurde zum Teil auf eine unmittelbare geschlechtsneutrale Schreibweise verzichtet.

Despite careful editing and production no guarantee can be given for the contents of this book. Any liability by publisher, editors and authors is expressly excluded.

Trotz sorgfältigster Bearbeitung erfolgen alle Angaben ohne Gewähr. Eine Haftung des Verlags, der Herausgeber und der Autoren ist ausgeschlossen.

Wissenschaftliches Redaktionskomitee

o. Univ. Prof. Dr. Gerhard Chroust
Univ. Prof. Dr. Gabriele Kotsis
Univ. Prof. DDr. Gerald Quirchmayr
Univ. Doz.  Veith Risak
Dr. Norbert  Rozsenich
Ao. Univ. Prof. DDr. Erich Schweighofer (Leiter)
o. Univ. Prof. Dr. Peter Zinterhof
Univ. Prof. Dr. Jörg Zumbach

Erich Schweighofer, Ahti Saarenpää, Janos Böszörményi (eds.)

KnowRiſht 2012

**Interaction of Knowledge Rights, Data
Protection and Communication**

25 Years of Data Protection in Finland

November 26 - 28, 2012

Helsinki, Finland

OCG Forum Privacy 2013

**IT Enterprises Between Surveillance State
and Consumer Responsibility**

October 09, 2013

Vienna, Austria

© Österreichische Computer Gesellschaft
Komitee für Öffentlichkeitsarbeit
www.ocg.at

Druck: Druckerei Riegel
1080 Wien, Piaristengasse 19

ISBN 978-3-85403-299-1

PREFACE

KnowRight conferences have been organized since 1995, always with regulation of the Knowledge Society as its main focus. The call for papers of KnowRight2012 put this as follows: “Traditionally KnowRight focuses on the interaction between Intellectual Property Rights, Information Rights, ethical issues, civil society and information technology.” This description is a telling example of how observations on the new societal significance of data protection and intellectual property rights have prompted a need to discuss the topic more broadly. This is the discussion we continued in the KnowRight2012 conference.

KnowRight 2012 at the University of Helsinki, Department of Social Research – Media and Communication Studies, was co-organised by the University of Lapland, Institute of Legal Informatics, the OCG Austrian Computer Society (Oesterreichische Computer Gesellschaft) and the ARI Center for Computers and Law, University of Vienna, jointly with the GI German Society for Informatics (Gesellschaft für Informatik), the Intellectual Property Law Institute of the Jagiellonian University in Krakow, and the DGRI German Society for Law and Informatics (Deutsche Gesellschaft für Recht und Informatik).

When the decision was made to hold KnowRight2012 in Helsinki, we saw a keener focus on the impacts of societal changes on legal regulation. While this was prompted by developments in society, it also had much to do with the Network Society (NETSO) project, hosted by the University of Lapland in Rovaniemi, Finland. The research in the project examined changes in society and the state using approaches and perspectives drawn from multiple disciplines. A major contribution of NETSO consists in the views of Latin America on privacy. Further, the OCG Forum Privacy Conference in October 2013 added the highly relevant topic of surveillance to this volume.

The world is changing. As such this is nothing new. What is new, however, is how rapid and surprising the changes can be. More and more often we must face the fact that what we know how to do and the ways in which we do it are no longer adequate. *Tacit knowledge*, traditionally a positive skill, rapidly becomes more of a liability.

Modern changes are often seen merely as technical changes, a good example being the transformation of mobile phones into ‘smartphones’. New technology and new operating systems combined to offer up a device used in a new way. Yet, there was far more going on here than met the eye. The transfer and sharing of information had changed significantly. This in turn is a striking reminder that our society is well on its way to becoming a network society, a society where we are dependent on information systems, information networks and many kind of terminal devices.

Terms, as Professor *Jaakko Hintikka* has so aptly noted, eventually meet their fate. And indeed it has become misleading to speak of the *Information Society*. We now live in the *Network Society*. We no longer have *E-Government* but *Information Government*. Information systems, terminals and information networks are now more than mere tools; and information is no longer just raw material.

Yet, there is more. In addition to the legislative reforms that often – but not always – accompany changes in technology, we have witnessed a change in the legal framework by which our society operates. In principle, the state has become – and in practice is becoming – a constitutional state, one built on the rule of law and legal planning. We find ourselves living in an age marked by a heightened respect for *fundamental* and *human rights*. Among other

developments, we have come to view the right to use information networks as falling into this category. This mind-set is wholly different to that which we saw back in the early days of Information Society, when the focus was on changes in the information and communications markets. In the Network Society, it is the rights of the individual that figure most prominently; the issues go beyond new technical capabilities.

All of the contributions to KnowRight2012 have been peer reviewed by the editors. This is not a typical set of conference proceedings. The volume includes articles from South America written as part of NETSO. The Network Society is increasingly a global society. Accordingly, international cooperation is a natural part of research in Legal Informatics. All of the parties involved gain from it. An Austrian contribution on surveillance was added with the OCG Forum Privacy 2013.

Throughout the conference a broad variety of topics was discussed. The scope included information society, data protection, electronic communication, IP law, digital rights and more. Also, the ongoing economic crises played a prominent role in some presentations.

Authors emphasized how the information society is changing democracy and discussed the challenges faced by legislation to mitigate risks deriving from our increasing independence on information networks and information. In light of the reform of the European Union's economic governance, the need for an enlightened debate about transparency, communication policy, democratic values of participation and the right to know was accentuated. Especially the importance of the right to information as a necessity for modern democracy was stressed. Beyond the notion information society, a shift to network society was identified, where it remains open, who, in fact, governs society. Finally, it was pointed out that to govern the network society, improvement of legislation and of tools available to legislators will be required.

In the data protection section the insufficient involvement of stakeholders in the governance of privacy and privacy impact assessments was criticized and parallels were drawn between the development and regulation of privacy and environmental democracy. Further, the right to privacy and the right to information were described as complementary rights which sometimes can collide, making necessary to evaluate relations between these two legally protected rights. It was also argued that access to information should not be restricted in fear that data protection or confidentiality of information cannot be guaranteed. Media and communications are caught between private and public interests, served by competition law and normative regulation respectively. Balance must be achieved between these interests. One of the authors addressed the issue by weighing the pros and cons for regulation and deregulation. Yet, in the information age e-communication and especially copyright law even intensify the problematic. Copyright law runs the risk to come into conflict with the freedom of expression.

In general, the digital revolution has brought numerous problems for the way copyright used to be regulated. These problems are the centrepiece of some of the contributions. On the one hand the discussions went back as far as the Roman Empire; on the other hand they included newest technologies. Legal and moral norms were examined. It was argued that new solutions need to be adopted and was pointed out that radical reform is needed to benefit from new technologies. A shift from a concept of reproduction to a concept of reutilisation was advocated.

As an additional perspective trademark rights were examined, with the suggestion to learn from successful solutions. The audience's attention was also pointed at the difficult issue of illegal distributing of music and cinematographic works as much as hyperlinks directing

internet users to protected works. As far as legal databases are concerned more focus on usability and improvement in design thinking was encouraged. General-purpose search engines should not become the prior point of access to legal sources.

The papers on digital rights examined a broad scope of topics. Possibilities were offered to make a democratic use of the internet. Legitimate use of personal data to enhance decision making processes was emphasised. The basic question, how to define the word “right” was discussed as much as the dynamic interaction of fundamental rights and the European Commission’s effort to use the digital environment to increase its influence. Different aspects of a person’s identity information were analysed, involving biometric applications but also identity theft.

Finland is a bilingual country. The national languages are Finnish and Swedish. Although the language of the KnowRight conference was English – in keeping with tradition – the volume includes two articles in Swedish, which are accompanied by English abstracts. These contributions provide insights into the research being done in Swedish on the conference topic and, at the same time, can be seen as a way of reaching out to our Nordic readership too. The summary of the OCG Privacy Conference 2013 is written in German with an English abstract.

Many persons worked to form the conference and to prepare the programme and the proceedings. Special recognition has to go to the work of the Programme Committee. The work of the Institute for Law and Informatics at the University of Lapland, the Department of Social Research - Media and Communication Studies at the University of Helsinki, the School of Communication, Media and Theatre at the University of Tampere and the Centre for Computers and Law of the University of Vienna deserve acknowledgement.

Last but not least, we have to thank the sponsors making this event possible: The House of the Estates and the University of Helsinki for conference facilities, the Office of the Data Protection Ombudsman, the National Audit Office of Finland and Castrèn & Snellman Attorneys for coffee breaks, lunches and receptions, the University of Lapland, NETSO project, for travel costs of invited speakers, and the OCG Austrian Computing Society for printing the conference proceedings.

Rovaniemi & Vienna, in March 2014

Ahti Saarenpää, Erich Schweighofer, Janos Böszörményi

PROGRAMME COMMITTEE

Reijo Aarnio, The Office of the Data Protection Ombudsman, FI (Co-chair - Local chair)

Jens Gaster, European Commission, EU (Co-chair)

Hannu Nieminen, University of Helsinki, FI (Co-chair - Co-ordinator, Local chair)

Tuomas Pöysti, National Audit Office, FI (Co-chair)

Ahti Saarenpää, University of Lapland, FI (Co-chair - Co-ordinator, Local chair)

Erich Schweighofer, University of Vienna, OCG & WZRI, AT (Co-chair - Co-ordinator)

Jon Bing, NRRCL, University of Oslo, NO

Peter P. Sint, OCG, AT

Alfred Büllersbach, Bremen, DE

Joseph A. Cannataci, University of Malta, MT

Danièle Bourcier, Bremen, DE

Gunter Ertl, OCG & Regional Court of Appeal (ret.), AT

Fernando Galindo, University of Zaragoza, ES

Lucie Guibault, University of Amsterdam, NL


Georg Jakob, FFII, DE

Albrecht Haller, Haller Solicitors, AT

Thomas Hoeren, University of Münster, DE

Philip Leith, Queen's University of Belfast, UK

Sybilla Stanislawska-Kloc, Institute of Intellectual Property Law, Jagiellonian University, PL

Alain Strowel, Facultés universitaires Saint-Louis et Université de Liège, Brussel 

Jos Dumortier, University of Leuven, BE

Dietmar Jahnel, University of Salzburg, AT

Benjamin Farrand, University of Strathclyde, Glasgow, UK

Judith Rauhofer, University of Edinburgh, UK

Eva Souhrada-Kirchmayr, Data Protection Commission, AT

Edgar Weippl, SBA Research, AT

TABLE OF CONTENTS

Preface	5
Table of Contents	11
Conference Programme KnowRight 2012	15
Conference Programme OCG Forum Privacy 2013	19
Introduction	
Legal Informatics Today	21
The View from The University of Lapland	
<i>Ahti Saarenpää</i>	
Data Protection in Finland	27
<i>Reijo Aarnio</i>	
OCG Forum Privacy 2013: An Overview	35
<i>Janos Böszörményi, Walter Hötendorfer</i>	
Information Society	
Information Policy and Citizens' Communicational Rights as Conditions for Sustainable Fiscal Policy in the European Union	43
<i>Tuomas Pöysti</i>	
The Management of Legal Documents in the Service of the Rule of Law	89
<i>Patricia Reyes</i>	
From 'Information' to 'Network' Society: What (if Anything) Has Changed?	97
<i>Marko Ampuja, Juha Koivisto</i>	
Regulating the Network Society	99
A Challenge for the Quality of Legislation and other Activities	
<i>Ahti Saarenpää</i>	
Surveillance Needs Transparency and Democratic Control	115
<i>OCG Forum Privacy – Coordinators:</i>	
<i>Walter Hötendorfer, Erich Schweighofer</i>	
Data Protection	
Public Voice in Privacy Governance: Lessons from Environmental Democracy	121
<i>Dariusz Kloza</i>	
Personal Data Protection and Access to Public Information:	149
Fundamental Rights for the Consolidation of Democracy	
<i>Laura Nahabetián Brunet</i>	
Habeas Data and Data Protection Law in Chile	161
<i>Romina Garrido Iglesias</i>	

Challenges of Increased International Data Exchange: Police/Security Services & Financial Transactions Erich Schweighofer, Walter Hötzendorfer, Janos Böszörményi	171
Electronic Communications	
Challenges of Convergence to European Media and Communications Regulation – A Model for Analysis <i>Hannu Nieminen</i>	181
Ebook and Access Rights <i>Anu Ojala</i>	191
IP Law	
Copyright and the Digital Environment <i>Niklas Bruun</i>	201
Privacy Friendly Remedies for Intellectual Property Rights <i>Mindaugas Kiskis</i>	209
Software Usability and Legal Informatics <i>Anna Ronkainen</i>	221
Linking and Copyright <i>Brita Kristina Herler</i>	229
Resolving the Crisis of Copyright Law in the Digital Environment: Reforming the “Copy-Right” into a “Reuse-Right” <i>Primavera De Filippi, Katarzyna Gracz</i>	245
On Scriptura, Printing and the Origins of Copyright <i>Mariagrazia Rizzi, Georg Jakob</i>	251
The Legal Principle of Fair Practice, Especially in the Paternity <i>Alfred Streng</i>	259
Digital Rights	
A Right to Knowledge and Information – and Subjective Rights <i>Wolfgang Mincke</i>	277
Identity Theft and the Finnish Identity Programme <i>Rauno Korhonen</i>	291
Democracy, Internet and Governance <i>Fernando Galindo</i>	301
Information Rights and other Fundamental Rights: Dynamic Interaction in the Changed Asylum System <i>Terhi Anttinen</i>	317
Categorizing Biometric Applications <i>Juhani Korja</i>	335

Legitimate Use of Personal Data in Credit Risk Assessment <i>Lorena Donoso Abarca</i>	347
The Production of Ideal Citizens in the Digital Agenda for Europe: A Narrative Perspective <i>Minna Saariketo</i>	361
Index of Authors	363

KNOWRIGHT 2012

CONFERENCE PROGRAMME

Monday, 26 November 2012
The House of the Estates

Plenary Session I, 9.00 – 12.00

Chaired by Erich Schweighofer

Opening & welcome, 9.00 – 9.15

Reijo Aarnio, Tuomas Pöysti

Keynote lecture I, 9.20 – 10.30

Law, Citizens' Communicational Rights and Disciplined, Responsible Fiscal Policy
Tuomas Pöysti

Coffee break, 10.30-11.00

Keynote lecture II, 11.00 – 12.00

Copyright Dilemmas in the Digital Environment
Niclas Bruun

Lunch, 12.00-13.30

Plenary Session II, 13.30 – 17.30

Chaired by Kaarle Nordenstreng

Keynote lecture III, 13.30 – 14.30

Locating What Isn't There in a Panspectric World
Sandra Braman

Coffee break, 14.30-15.00

Keynote lecture IV, 15.00 – 16.00

Challenges of convergence to European media and communication regulation: towards an analytical framework
Hannu Nieminen

Keynote lecture V, 16.00 – 17.30

Data Protection Reform - are we ready? - 25 years of Data Protection in Finland
Reijo Aarnio

Cocktails, 18.00-19.30, The House of the Estates

Tuesday, 27 November 2012
University of Helsinki

Plenary Session III: 9.00-10.00

Chaired by Fernando Galindo

Keynote lecture VI, 9.00 – 10.00

Protection of data as an everyday fundamental right

Ahti Saarenpää

Coffee break, 10.00-10.30

Session I.A: Governance questions, 10.30 – 12.00

1. Governance by design in distributed architectures

Primavera de Filippi, Danièle Bourcier

2. Democracy, Internet and Governance

Fernando Galindo

Session I.B: Finnish studies on media law, 10.30 – 12.00

1. Knowledge workers in the Finnish information society

Tiina Saari

2. The production of ideal actors in Digital Agenda for Europe: a narrative perspective

Minna Vigren

3. (R)evolution of Freedom of Speech Doctrine in Finland

Riku Neuvonen

Lunch, 12.00-13.00

Session II.A: IP law I, 13.00 – 14.30

1. Software Usability and Legal Informatics

Anna Ronkainen

2. Privacy friendly remedies for intellectual property rights

Mindaugas Kiškis

3. Copyright law in the digital era: the failure of an autopoietic system

Primavera De Filippi, Katarzyna Gracz

Session II.B: Panel discussion, 13.00 – 14.30

Panel: Data Breach - what to do?

Nicklas Thorgerzon, Eija Warma

Coffee break, 14.30-15.00

Session III.A: Data Protection I, 15.00 – 16.00

1. The public voice in privacy impact assessment: what could be learnt from international environmental law?

Dariusz Kloza

2. Challenges of increased international data exchange

Erich Schweighofer

Session III.B: Patents & IP law, 15.00 – 16.00

1. The Unitary Patent and the European Patent Court - a Report from the Deathbed

Benjamin Henrion

2. Mapping the Patent Wars: Retrieving and Visualizing Patent Information
Georg Jakob
3. On the Origins and History of Copyright
Mariagrazia Rizzi & Georg Jakob

Cocktail party for foreign speakers, 17.00 - 19.00 Castrèn & Snellman Attorneys

Wednesday, 28 November 2012
University of Helsinki

Session IV.A: IP law II, 9.00 – 10.30

1. EU Patent Reform
Jens Gaster
2. The "Dominance" in Abuses of Dominant Companies
Aleksander Wiatrowski
3. Networking and acquisition of future copyrights
Alfred Streng

Session IV.B: Data protection II, 9.00 – 10.30

1. A right to know and subjective rights
Wolfgang Mincke
2. Data Protection and the Re-use of Public Sector Information in the European Union
Dino Girardi
3. Identity Theft and the Finnish Identity Program
Rauno Korhonen

-- Coffee break, 10.30-11.00

Session V.A: Interdisciplinary questions, 11.00 – 12.30

1. Categorizing biometric applications
Juhani Korja
2. Freedom of speech and copyright in eBook contracting
Anu Ojala
3. Right to information within the European Asylum System
Terhi Anttinen

Session V.B: Finnish studies on media law, 11.00 – 12.30

1. From 'Information' to 'Network' Society: What (if Anything) Has Changed?
Juha Koivisto, Marko Ampuja
2. Website Blocking Injunctions Imposed on ISPs: Constitutional Lessons for EU Law-Meets-Internet Research
Lassi Jyrkkio

Closing session, 12.30-13.00

Ahti Saarenpää, Erich Schweighofer

OCG FORUM PRIVACY 2013
CONFERENCE PROGRAMME
IT-UNTERNEHMEN ZWISCHEN
ÜBERWACHUNGSSTAAT UND
KUNDENVERANTWORTUNG
(IT ENTERPRISES BETWEEN SURVEILLANCE
STATE AND CUSTOMER RESPONSIBILITY)

A conference of the the OCG Forum Privacy in co-operation
with the Austrian Trade and Industry Association
(Gewerbeverein)

Wednesday, 9 October 2013, 09:30 to 17:00
Location: Österreichischer Gewerbeverein, Eschenbachgasse 11,
Beletage, 1010 Vienna

The event was professionally filmed. The videos are available on YouTube:

<https://www.youtube.com/playlist?list=PLFs9xVyHU-keZNL4CbhdM4Mt5IMueiOrX>

9:30 - 10:00 Opening & Welcome Statements

Ronald Bieber, General secretary of the Austrian Computer Society (OCG)

Christof Tschohl and **Walter Hötendorfer**, both heads of OCG Forum Privacy

Hannes Tretter, Professor & Co-chair of Ludwig Boltzmann Institute of Human Rights

Max Mosing, Solicitor & Vice-president of IT-Law.at Association

10:00 - 10:30 *Aktueller Stand der Enthüllungen zu den geheimdienstlichen*

Überwachungsaktivitäten und Diskussion in Europa (*Up-to-date of revelations on secret service surveillance activities and discussion in Europe*)

Andreas Krisch, Chairman VIBE.at, President European Digital Rights

10:30 - 11:00 *Unternehmensverantwortung im praktischen Spannungsfeld: Schilderung aus der Sicht von Unternehmen, die staatlichen Anfragen zur Speicherung und Herausgabe von Nutzerdaten ausgesetzt sind* (Enterprise responsibility in a practical area of conflict: Description from the perspective of enterprises that are exposed to requests by state authorities to retain and disclose user data)

Maximilian Schubert, General Secretary ISPA – Internet Service Providers Austria

Maximilian Schubert, General Secretary ISPA – Internet Service Providers Austria

11:00 - 11:30 Coffee break

11:30 - 12:00 *Völkerrecht: **Multinationale IT-Unternehmen** zwischen widersprüchlichen rechtlichen Anforderungen diesseits und jenseits des Atlantiks (International law: transnational IT enterprises between conflicting legal requirements on this side of and across the Atlantic)*

Erich Schweighofer, Professor and Head of the Centre for Computers and Law, Section for International Law, University of Vienna; President of the WZRI Vienna Centre for Legal Informatics

12:00 - 12:30 *Unter dem Radar der NSA - Überblick über die wichtigsten geheimdienstlichen Methoden und Technologien (Under the NSA's radar – an overview of the most important secret service methods and technologies)*

Erich Moechel, ORF.at Journalist and IT expert

12:30 - 14:15 *Lunch break*

14:15 - 14:45 ***Industriespionage in der Public Cloud: Gefährden PRISM & Co auch die Geschäftsgeheimnisse europäischer Unternehmen?** (Industrial espionage in the public Cloud: Do PRISM and other programmes also endanger the business secrets of European enterprises)?*

Gert R. Polli, former Head of the Federal Office for the Protection of the Constitution and Counterterrorism, CEO Polli GmbH - Intelligence & Public Safety

14:45 - 15:15 ***Wie kann und soll die Politik in Österreich und der EU auf die bekannt gewordenen Überwachungsaktivitäten reagieren?** (How can and should politics in Austria and the EU react to the learnt surveillance activities?)*

Waltraud Kotschy, former Head of the Austrian Data Protection Commission, legal adviser, external data protection expert for the BIM Ludwig Boltzmann Institute of Human Rights

15:15 - 15:45 *Coffee break*

15:45 – 17:00 **Panel discussion** on the event's topic with interactive audience participation

LEGAL INFORMATICS TODAY

THE VIEW FROM THE UNIVERSITY OF LAPLAND

Ahti Saarenpää

Professor of Private Law, Chair in Family law, Law of Inheritance and Law of Personality
Director of the Institute for Law and Informatics, Faculty of Law University of Lapland
Vice-chairman of the Data Protection Board, Finland.
asaarenp@ulapland.fi

Keywords: *Legal informatics, information law, network society, legal welfare, data protection, information government, access*

Abstract: *The society we live in is changing; and the state we live in is changing. This has always been the case. In recent years, the pace of such peaceful changes has quickened. Our society is changing apace into a Network Society and the state is becoming a full-fledged constitutional state. These simultaneous changes are challenging for legislators and Law alike. We face a pronounced risk that legislation and Law will not keep pace with change. Legal Informatics can with good reason be characterised as a science of change. From its very inception, scholars in the field have deliberated the opportunities which the use of IT has brought to society. Today the focus is shifting to the risks which that development poses to our enjoying our human and fundamental rights. We are increasingly dependent on information networks and information. We and others process information and, at the same time, engage our fundamental rights in a digital environment and on information networks. In a word, we are witnessing an information revolution of sorts, one where it is expected that the rights of the individual are acknowledged and accommodated early on in legal processes. This can be ensured to a considerable extent through sound legal planning of information systems. The KnowRight conference is a multidisciplinary forum whose focus is changing. Yet, all the organisers of the conference work in the field of Legal Informatics. As the meeting is being held in Finland this time, it is important to present modern Legal Informatics from a Finnish perspective.*

As one of the legal and communication sciences, Legal Informatics is very much a science concerned with change. It has already been one for a long time. 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 interest. Gradually they changed to become 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.

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. It was no surprise then that Professor *Peter Blume* noted in his inaugural lecture in Copenhagen that subject imperialism in our university life had prevented us seeing the 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.

Today we no longer live in the Information Society. That era is 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. 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 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.

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 distrait 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 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 my 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 training in the field, this change in perspective 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.

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: (1) Legal Information, (2) Legal Data Processing, (3) Information Law and (4) ICT Law. We plan to continue our research and to teach within this framework, although its 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. This 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.

At the same time, the relationship between Information Law and 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 Professors *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, Professor *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 professor *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.

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 Legal Informatics 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, Mr. *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 cyber- security 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 in 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.

DATA PROTECTION IN FINLAND

ANNUAL REPORT 2012

Reijo Aarnio

Data Ombudsman, Doctor h.c.
Office of the Data Protection Ombudsman
P.O. Box 800, 00521 HELSINKI, FI
Reijo.Aarnio@om.fi; <http://www.tietosuojafi/1560.htm>;

Keywords: *Data protection, basic rights, supervisory authorities, data security, sector surveys*

Abstract: *The 25th year of operations of the Data Protection Ombudsman was particularly important because, on 25 January in our silver jubilee year, the European Commission submitted its proposed total renewal of data protection legislation. Over the course of time, cases have become even more complex because traditional register management has become application-based personal data processing which is increasingly often affected by a strong supranational element. At the same time the shortage of skills in society is unfortunately still glaring.*

1. Introduction

Development has been immense in the past years. *Johanna Tornberg*, LL.D., who completed her dissertation at the University of Lapland, described the change in society as follows: citizens are moving away from their role as being subordinates to administration, and they are becoming customers. Basic legal thinking emphasizes the sovereignty of the individual. On the other hand, basic rights and privacy and personal data protection have become more horizontal. The basic fundamental rights which the government shall actively promote and which must be accounted for ex officio in the operations of the authorities have an impact on all legal relationships, not only on the relationship between the government and the citizens. In this context, it is worth noting that the purpose of the Finnish Personal Data Act and the related general Data Protection Directive is also to protect other basic rights than just the right to privacy.

At the same time, information (i.e. data) has a new societal meaning. We have learned to evaluate data from the perspective of processes. As the amount of data continues to grow (*big data*) and its quality changes (*open data*), we have learned to consider data as capital and a production factor. Data is a powerful thing, but more and more often we hear slogans such as "personal data keeps the economy moving", or "privacy is dead". The challenges brought about by technology, in particular, have been regarded as justifications of the latter slogan. In legal science, data rights should be playing an increasingly important role. At the same time the shortage of skills in society is glaring.

The *European Commission* published its status evaluation as the EU shifted from the fifth framework programme to the sixth. In the evaluation, the Commission required that data protection management be an active part of the system design of data systems and services. It also required that data protection support IT infrastructure be created in Europe. According to the Commission, financial activity should be promoted by developing new approaches to online data protection and business models would have to be renewed to ensure data protection. For some reason, development has not been as fast as required by the Commission.

The Office of the Data Protection Ombudsman in Finland has performed extensive visionary and strategy work. Our resources do not increase at a pace equal to the increase in demands and challenges. We need to be increasingly effective. At the same time, *managing human capital* at the level of our organization is an even more important tool.

The Commission's new "package" includes two parts: a proposed regulation which would replace the current general data protection directive (95/46/EC), and a directive to replace the framework decision approved for the third pillar. However, this is actually part of a bigger framework: to establish a genuine digital internal market, the Commission has also proposed that European consumer protection be renewed and a European commercial law be enacted. Money from Europe, struggling with the financial crisis, is leaking to third countries. Finally, people are beginning to understand that data protection is a *success factor*.

When approved, the proposal would provide the Office or another party with many new core processes, such as authority to perform advance inspections, to process notifications to the authorities related to data infringement, to have the authority to impose fines, etc.

According to paragraph 3 of Article 8 of the Charter of Fundamental Rights of the European Union (2010/C 83/02), part of the Treaty of Lisbon, which defines the EU, compliance with personal data protection rules is controlled by an *independent* authority. This means that the status and independence of the data protection authorities is strong enough. The status and related tasks are described by the general data protection directive (95/46/EC) such that within the area of each Member State, compliance with the directive and national legislation is controlled by one or more public authorities. According to Article 28 of the directive, the authorities must perform their tasks independently.

In Finland, in addition to the general judicial power of the Data Protection Ombudsman and the Data Protection Board, the Finnish Communications Regulatory Authority (FICORA) also participates in the control of data protection by the authorities (based on the national implementation of the electronic communication data protection regulation (2002/58/EC) as do the occupational safety and health authorities in regard to the law regarding data protection in working life. However, the Finnish arrangement, which has worked well, in my experience, raises some questions related to the overlap in authority regulations and to the independence of the operations of the authorities. The monitoring of the *Schengen Agreement* is an example of the latter question. During my service the independence of the Ombudsman has already been evaluated three times as required by the procedure set out in the Agreement. As far as I know, similar evaluations have not been performed for the other agencies mentioned above. The main question is related to the consistency of decisions. Naturally, I am worried about scenarios where we, the authorities, may provide mutually conflicting interpretations of the data protection legislation.

This de facto independence of the data protection authorities is further emphasized in the Commission's proposal for a new data protection regulation. According to Article 47 of the proposal, Member States must ensure that an independent or (due to the national approach) independent law enforcement authorities are provided with sufficient technical, financial and personnel resources, facilities and infrastructure, which are needed to effectively perform the required tasks and exercise the necessary authority. According to the proposal, the controlling authority must also have its own, separate, public budget.

More extensively speaking, the law enforcement machine also includes data protection officers and, perhaps surprisingly to many, the police. Data protection officers, already identified in Finnish law in regard to specific sectors, have a large responsibility for ensuring that the self-guidance principle of data protection legislation is followed. On the other hand, the police are the competent authority to use prejudicial inquiry-related enforcement in regard to data protection crimes. The police also control a significant amount of data.

Finnish law says that the Ombudsman must be heard when prosecutors and courts of law process crimes related to personal data protection and the confidentiality of communication. The number of hearings has steadily increased year by year. At the moment, Finnish courts of law process several data protection crimes every week. On the basis of our reviews of the sanction system, they usually lead to rather minor fines. However, in addition to the low level of sanctions, the allocation of the sanction system is a major concern to me. People working for registrars have been convicted of data protection offences. At the same time, it seems that the action taken by the registrar organization is not focused enough. In other words, it is imperative that in Finland, too, it would also be possible to impose sanctions on organizations in addition to individuals.

It is especially worth noting, and also underlining the prevailing situation, that in the proposed regulation, personal data protection has been "elevated" to a separate right. This means that it is being separated from privacy protection, often emphasized too much in Finland, and becoming a separate object of legal protection.

The observation is particularly significant in regard to transatlantic relations. The U.S. system, or the system adopted in APEC, underlines "Privacy". This involves a paradigm where the processing of personal data is allowed if it does not cause any harm to the registered person. In Europe, personal data protection is defined in a strong way, based on information-related autonomy. When drawing up their first data protection laws, many countries vacillate between the two approaches. For the legal protection of the registered people, it is mandatory in the first phase to create at least some kind of mechanism which intends to combine the two systems.

2. Activity

The Commission's proposal includes, for instance, a proposal on a "consistency mechanism", meaning a legal instrument aiming – like the entire reform – at better harmonization of data protection and the creation of a genuine digital single market in the EU. In such cross-border data protection issues, the decision-making would take place in a new EU Data Protection Board to be established. However, since the majority of such cross-border issues already seem to be "local" Nordic issues, we have already practiced using the instrument with our Nordic colleagues.

Nordic cooperation has also otherwise become deeper and sharper, which is nice. We help each other in strategic and operative planning and functions and have successfully made our cooperation practical. In believe that joint Nordic inspections are here to stay. The cooperation on the presenter and expert levels is also deep. Perhaps in this theme, too, we can also set an example to many others.

In November 2011, Finland was faced with a barrage of hacking attacks. Did we learn anything about these security breaches? We tried to answer this question during the year under review by conducting an extensive survey of the parties that had been attacked by hackers. We aimed to find out what kind of problems the security breaches caused and what kind of measures the organizations took to correct the situation. The outcome was quite dispiriting. Breaches of security at small-scale companies and organizations, for example, directly caused hazards to the organizations' operating continuity; because many small-scale actors had to completely stop their online services due to the infringement. The other extreme was constituted by targets in the review who found that they had no need whatsoever to improve their data security. A stunning 30 per cent of the respondents were like this, thinking that lightning never strikes the same place twice! Section 32 of the Personal Data Act requires that registrars take the necessary data security measures to protect the personal data of their customers. Only 46% of the respondents reported that they were aware of this stipulation. It is necessary to enact a general data security act in Finland.

When preparing for the above-mentioned survey, we arranged an extensive workshop on data security as part of the 25th anniversary of our office. During this workshop, the guests – consisting of experts in the sector – were posed two questions: 1). Is there any need to improve data security in Finland? 2). If so, is there sufficient expertise in the country to achieve this? Examples of views:

- The opportunities for misuse have increased to a great extent and misuse is simply too easy in our online society.
- Personal data is used incorrectly. For example, it is unfortunately often the case that the social security number, intended to separate personal data from each other, is used for identification.
- Personal data is used online to commit traditional frauds. As such, personal data is valuable for criminal purposes.
- Biometric identifiers are stored in digital format in data systems. Now that systems seem to leak, data based on permanent biometrics will leak unless it is successfully protected.
- Our national regulations and the currently available system of sanctions are insufficient.
- There is no contact point where citizens can get assistance. It just does not exist.
- The obligation to give notice of data security infringements and threats should be expanded to apply to all registrars.

Unfortunately, the guests' reply to the first question was "yes", and they answered "no" to the second. Fortunately, Finland has drawn up its first strategy to protect against cyber threats. To improve the accountability of the executives of organizations, we published the accountability guide. Perhaps it will also help organizations to use the modern approach of data management.

In addition to the above-mentioned workshop, workshops on telephone directory business, social media (whether there are 'grey areas' that the authorities cannot govern in social media), voluntary operational control and data protection for entrepreneurs were arranged during the year under review. The anniversary year culminated in a conference in Finland called KnowRight2012 which we were involved in.

Particularly in regard to social media, the discussion also included the entire social media value chain in addition to my aforementioned evaluation of official authority. The traditional way of assessing the data work value chain has been to start with content production and package it based on the needs of the customer. The packaged content has then been transferred to the paying customer. Now this approach has been turned on its head: social media users themselves produce the content and transfer and publish it. This means that customers have become users and advertisers have become customers.

Teleoperators are naturally following the example of social media and new technology. The boom in smartphone use, which has led to free access to different data transfer services and instant messaging applications, has challenged the earning logic of operators. The sales of ad-funded subscriptions have, at least partially, solved the issue. However, the data protection act concerning digital communication requires the registered person to opt in before marketing is possible. In the law, consent is defined as a unilateral, voluntary, data-based recognition of will, which the registered person should be able to cancel without any negative repercussions. Consumer protection authorities were facing a difficult problem: can required consent be a contract term? The earning concept still remains under review.

These things go hand in hand: how can we then keep advertisers or application developers happy? We have thus ended up to addressing a key question regarding data networks and Internet society as a whole: should there be net neutrality, or should some people be granted priority on the data high-

ways? Information networks still have a limited amount of bandwidth available. As the current move to the IPv6 system of IP address numbering progresses further, the networks will become more congested. Who will be left behind?

A somewhat similar consent-related question was encountered in regard to academic research. The question was also raised of what should be done with already collected material containing sensitive personal data if and when the person included in the study cancels their consent. The researchers were worried that the quality of the material would be harmed. We proposed that consent should be the justification for processing personal data, and the processing should end when that consent is cancelled. However, it should be possible to retain material obtained before then.

As the Council of Europe was drafting a recommendation on profiling, we published a sector survey on regular customer systems, which was implemented early in the year.¹ We found that the legal quality of regular customer systems varies to some extent. Some of the respondents could not say why they use a regular customer system. Following that, there were incidents which caused food safety hazards. Toxic olives made it past the quality control systems of stores and the food authority, and later there also were other products which caused health hazards to consumers. The food safety authority stated that loyalty card system data be merged with cash register system data to allow consumers who had purchased toxic products to be traced. The measure was successful in regard to the fact that the issue did not escalate. What about responsibility? I have heard of a case of mad cow disease in the United States where the store managing the loyalty card system didn't react in the manner described above, which meant that customers' lives were put at risk due to the store's failed QA system and poor information management. Perhaps the lesson to be learned is that questions of responsibility related to using such, often large, personal data systems, are becoming increasingly important.

3. Policies

At the request of the Data Protection Ombudsman, the *Data Protection Board* commented on the strong identification system required in some booking systems. The case referred to the legal quality of an online service of a chain of optician's stores where people booked appointments and implemented other actions using their name and social security number. The Board agreed with the Ombudsman's statement that the system in question is not secure enough and that social security numbers were being used to separate people from each other in databases. The controller in question has started to modify the system. We were happy with the policy specified by the Data Protection Board but had to consider the current shape of the infrastructure of our online society. It seems that the decay has started even before the infrastructure is completed.

At the request of the Data Protection Ombudsman, the Data Protection Board studied CCTV monitoring in the stairwells of residential buildings as an important matter of principle. The case referred, among other things, to the link between the Personal Data Act and the Criminal Code of Finland. The Board stated its opinion that CCTV monitoring is possible in these facilities based on the stipulations of the Personal Data Act.

The Data Protection Ombudsman also referred to the Data Protection Board cases regarding exercising rights of access and credit information. In the first case, the main question was whether the right of access, as required by the Ombudsman, should also be possible by means of an electronic signature. The latter case refers to the way the information in credit information registers is used, its availability in the manner regulated by the Credit Information Act, and the correctness of the information provided to the people registered.

¹ The *sector survey* is a tool we have developed. Its goal is to make inspection activities as efficient as possible utilizing technological means.

Partly due to the lack of comprehensive legal praxis, the Ministry of Transport and Communications ordered a survey of the legislative status of digital estates from *Urpo Kangas* of the University of Helsinki (an expert in inheritance law). The original phrasing of the question concerned the right of the next of kin to obtain a deceased person's email correspondence but, as the review progressed, the phrasing extended and became increasingly general. One of the conclusions of the report was that more specific legal regulations should be made in regard to digital estates. In this respect, it is easy to agree with the recommendation. However, the author's idea that basic rights and particularly data protection rights (and registrar's obligations) would end at death is not familiar to our data protection system and, as far as I know, to basic legal thinking in a more general way. The Finnish government proposal on the Personal Data Act addresses the question of protecting the personal data of a deceased person as follows: "The proposal would not expressly include stipulations on protecting the privacy of unborn children or the deceased ... The application procedure of the act – Personal Data File Act - finds that the act also applies to the deceased ... it is found that the privacy protection need provided by the Personal Data Act also decreases when data is collected on those who have died a long time ago."

We know that a biobank in our neighboring country went bankrupt. More and more providers of digital storage services have just announced that they are ceasing their activities. We, the consumers, more and more often store our digitized documents and data, such as X-ray images or holiday photos, behind our username and password in the cloud. It seems that very few people really know what the hype is all about. In many cases, cloud services are reviewed on the basis of personal data migration-related regulations. That kind of review is far too narrow because it does not sufficiently account for the legal protection of the registered person.

The digital estate in regard to physicians and patients may include sensitive personal data. My view has always been that providers of services which involve sensitive personal data, or personal data subject to confidentiality regulations, must adhere to a particularly high level of data security. Not everyone agrees. The Deputy Parliamentary Ombudsman – following my opinion – criticized a healthcare provider for using an insecure email connection when communicating with patients. This raised a storm in a teacup. The decision was criticized because it was "a leap to the stone age" and described "how alienated the authorities are from real life". It seems to be almost always difficult to communicate serious data protection matters!

Banks, with their long tradition of processing personal data and adhering to bank secrecy, have resolved this by providing their customers with a secure interface based on online banking. The system identifies the customers in a strong way, messages are encrypted during transfer, and the system includes many data security elements. The lesson to learn is that, at least in connections in Finland, our financial information is protected better than our sensitive patient data.

What action have lawyers in Finland taken in regard to data security requirements? As far as I am aware, the *Finnish Bar Association*, which provided its members with a secure e-mail service, has shut down this service! However, I am glad that we have had the opportunity to engage in closer cooperation with the Association in regard to training events and communication provided for their members. I have also found that important because, in my view, registrars will more and more frequently consult agencies that are familiar with information legislation. Among lawyers, I have identified signs that business approaches based on genuine data protection are being introduced.

4. Plenty of interesting developments

During the year, a continued legislation project under review was the compilation of 'an information society code'. Our office also participated in the work of the steering group and specific subgroups, whenever possible. In my opinion, parties acting in the digital economy and service production have difficulties in finding legislation to guide their operations, mainly due to the fragment-

ed nature of the legislation.² This is one of the reasons why the parties active in the sector may be unsure and uncertain, which in turn may hamper development.

One important reform that received fairly little attention was the implementation of employee tax numbers. In Finland, each person is issued a personal identity code (HETU), which is entered into the Population Register, and an electronic client identifier to be used when dealing with the authorities (SATU). Furthermore, the Tax Administration has now implemented a tax number issued to all employees, in an attempt to curb the grey market. At least in this respect, the public administration, pleasingly, seems to be able to manage risks pertaining to managing identities. On the other hand, the development of mobile services based on SATU has had a fairly slow start.

However, it is clear that developments in the European digital internal market will need some kind of joint understanding on matters related to identity management. Will we someday have to introduce a joint European personal identity code, or will we go for an option based on the decentralization of risks? I believe that a solution will soon be urgently needed because, as far as I am aware, major international operators are seeking business based on identification services. It may be that a situation is emerging in which the same operators have a dominant position in identity management and identification services, communication services and application-based services based on the location of the registered person.

Another step forward by the public administration is the development regulated by the public data administration act³ that entered into force in 2011: control over the utilization of information technology has been further centralized to the decision-makers of state-owned enterprises. One of the proposals issued over the course of the year was to establish an IT service company owned by the State. The national *auditing* based on the data security regulations seems to have started well.

The Office of the Data Protection Ombudsman participated in the control of the above-mentioned issues and the control of scientific research, supervision of DNA sample collections, issues pertaining to intelligent transportation systems and road tolls, communication on threatening data leaks from smart phones, reform of the Act on Processing of Personal Data by the Police, the work of the Human Rights Centre⁴, and many other projects. In addition to our intensive daily work, we must be able to create wider perspectives. Part of this broader point of view comes from the currently ongoing extensive European and Nordic cooperation, while part comes from participation in *NETSO*, a project funded by the Academy of Finland and led by Professor *Ahti Saarenpää* that horizontally studies the development of the information society.⁵

Data protection is at the start of a new age. This will impose considerable challenges for the service capability of our Office. At the moment, the Office annually receives almost 4,000 cases in writing. The demand for our phone service is also high. The Data Protection Ombudsman is authorized to resolve inspection, error correction and refusal right matters. The number of these has remained quite steady, at about 200 cases per year. Instead, the number of advance notifications, general inquiries and forward requests has increased rapidly. Unfortunately, the number of crime-related cases is also steadily increasing. A particularly pleasant task is to participate in committee work related to legislation projects, and to be invited to be heard by parliament. A specialty of ours comprises sector reviews performed by us, where we intend to have a maximum societal impact by our inspection operations.

² An example of this is a government proposal regulating the use of biometrics in the Radiation Act that was being processed by the Parliament. There is no specific Finnish act on biometrics.

³ Act on Information Management Governance in Public Administration.

⁴ The Human Rights Centre promotes fundamental and human rights. It is functionally autonomous and independent, but administratively part of the Office of the Parliamentary Ombudsman.

⁵ The name of the research project is *Network Society as a Paradigm for Legal and Societal Thinking* (NETSO).

Over the course of time, cases have become even more complex because traditional register management has become application-based personal data processing which is increasingly often affected by a strong supranational element. That is why we constantly strive to develop our skills and our capability to pass them on. I am still very proud of the performance of my long-term and short-term colleagues in this regard.

OCG FORUM PRIVACY 2013: AN OVERVIEW

Janos Böszörményi, Walter Hötendorfer

Ph.D researchers, University of Vienna, Centre for Computers and Law
Schottenbastei 10-16/2/5, 1010 Vienna, AT
janos.boeszormentyi@univie.ac.at; walter.hoetendorfer@univie.ac.at;
<http://rechtsinformatik.univie.ac.at>

Keywords: *Surveillance state, customer responsibility, Austrian Computer Society, OCG Forum Privacy, Edward Snowden, data retention, NSA, PRISM, GCHQ, TEMPORA*

Abstract: *In light of the revelations made by Edward Snowden, the OCG Forum Privacy, a working party of the Austrian Computer Society (OCG), hosted a conference on 9 October 2013 in Vienna. The conference was co-hosted by IT-Law.at, Ludwig Boltzmann Institute for Human Rights (BIM) and Vienna Centre for Legal Informatics (VCLI). The centre piece of numerous surveillance practices, which were revealed by Snowden, is the access of state authorities to the user data of private companies. These private companies, above all “Big Players” such as Google and Facebook, face conflicting obligations towards governments on the one hand and responsibilities towards their customers on the other hand. To address this area of conflict, the conference was held under the title “IT companies between surveillance state and responsibility to the customer”. After an overview of surveillance techniques was presented by Andreas Krisch, Maximilian Schubert from the Austrian association of Internet Service Providers gave an insight into practical issues for businesses. Erich Schweighofer explained aspects of surveillance related to international law and Wolfgang Schwabl discussed actual methods of surveillance. Erich Möchel, Gert R. Polly and Waltraut Kotschy addressed a variety of further aspects and recent developments from a technical and a legal perspective. The slides and video footage of all presentations and of the final plenary discussion are available at http://www.ocg.at/privacy_business.*

1. Einleitung

Unter den Eindrücken der Snowden-Enthüllungen veranstaltete das OCG Forum Privacy, einer der Arbeitskreise der Österreichischen Computer Gesellschaft (OCG), am 9. Oktober 2013 eine Tagung in Wien. Mitveranstaltet wurde die Tagung von IT-Law.at, dem Ludwig Boltzmann Institut für Menschenrechte und dem Wiener Zentrum für Rechtsinformatik. Kern vieler der von Edward Snowden enthüllten Überwachungspraktiken ist der Zugriff auf Nutzerdaten privater Unternehmen durch staatliche Behörden. Diese Unternehmen, allen voran „Big Player“ wie Google und Facebook, stehen somit in einem Spannungsfeld zwischen ihren diesbezüglichen Pflichten den Regierungen gegenüber auf der einen Seite und Ihrer Verantwortung den Kunden gegenüber auf der anderen Seite. Dieses Spannungsfeld griff die Tagung mit dem Titel „IT-Unternehmen zwischen Überwachungsstaat und Kundenverantwortung“ auf. Die Präsentationsfolien und Videos aller Vorträge und der abschließenden Podiumsdiskussion sind unter http://www.ocg.at/privacy_business verfügbar.

2. Begrüßung

Die gut besuchte Veranstaltung in den Räumlichkeiten des Österreichischen Gewerbevereins wurde von **Ronald Bieber**, Generalsekretär der Österreichischen Computergesellschaft (OCG), eröffnet. Er wies darauf hin, wie wichtig das Forum für die OCG sei und betonte die Aktualität von Themen wie Datenschutz und Privacy. Siebzig Prozent der großen deutschen Unternehmen seien bereits von Hackern angegriffen worden, wobei ein Schaden in der Höhe von Millionen von Euro entstanden sei.

Anschließend begrüßte **Walter Hötendorfer** das Publikum, der das OCG Forum Privacy gemeinsam mit **Christof Tschohl** leitet, und übergab das Wort schließlich an diesen, der durch das Programm führte. Tschohl berichtete eingangs in seiner Rolle als Gründungsmitglied des Arbeitskreises Vorratsdatenspeicherung (AKVorrat.at) über die Klage des AK Vorrat gegen die EU-Richtlinie zur Vorratsdatenspeicherung und verzeichnete positiv, dass das Gewicht des Themas und dessen öffentliche Wahrnehmung sich geändert habe. Zum ersten Mal seien nicht mehr die Kläger in der Defensive, sondern der Rechtfertigungsdruck liege bei den Befürwortern der Vorratsdatenspeicherung.

Begrüßungsstatements von **Hannes Tretter**, Co-Leiter des Ludwig Boltzmann Institut für Menschenrechte und **Max Mosing**, Vertreter der wissenschaftlichen Interessengemeinschaft IT-Law.at waren geplant, allerdings fiel Hannes Tretter kurzfristig aus. Rechtsanwalt **Max Mosing** erläuterte zunächst den Anwesenden die Tätigkeit von IT-Law.at. Dieses wurde 2001 gegründet und hat 185 Mitglieder. Auf die Website, die 169 Publikationen enthält, wird monatlich 2.500-fach zugegriffen. In der Folge erinnerte er an seine Publikation beim IRIS2003: „Nach 9/11 – Die Zukunft des Datenschutzes“. Das Thema sei jetzt ganz aktuell auf dem Tisch, es habe aber niemand darüber gesprochen bis Snowden an die Öffentlichkeit ging. Das Problem des Datenschutzes sei, dass die einzelnen Daten für sich genommen unbedeutend erschienen. Er bemängelte, dass Strafen für Unternehmen zu gering, und die Kosten für Compliance hoch seien.

Nachfolgend werden in je einem Kapitel die auf der Tagung gehaltenen Vorträge kurz zusammengefasst.

3. Aktueller Stand der Enthüllungen zu den geheimdienstlichen Überwachungsaktivitäten und Diskussion in Europa

Andreas Krisch, Obmann VIBE.at, Präsident European Digital Rights

Andreas Krisch begann mit einer historischen Rückblende. Die Überwachungspartnerschaft USA-UK wurde durch Australien, Kanada und Neuseeland zu den Five Eyes erweitert. Die Existenz des Echelon-Programmes zur Überwachung von Satelliten-Kommunikation wurde bereits 2001 durch das Europaparlament festgestellt. Heute werden Telefondaten in den USA systematisch – auf Anordnung des geheimen FISA-Gerichtes – überwacht. Das PRISM-Programm ermöglicht den direkten Zugriff auf Daten – auch Inhaltsdaten – der Nutzer bei großen Anbietern. Die Überwachung erfolgt in Echtzeit. US-Bürger dürfen nicht überwacht werden, weil der Geheimdienst nur im Ausland tätig sein darf, wahrscheinlich werden sie aber trotzdem überwacht. Deutschland ist eines der Hauptziele der Überwachung. Das vom britischen Geheimdienst GCHQ betriebene TEMPORA-Programm spezialisiert sich auf das Abhören von (Unterwasser-)Glasfaserkabeln. Es hat Zugang zu mehr als 2000 Glasfaserkabeln und kann gleichzeitig bis zu 46 davon abhören. Das US-Äquivalent zu TEMPORA ist das von der NSA betriebene Upstream. Daten nehmen den billigsten, nicht den kürzesten Weg. Daher kann man dafür sorgen, dass möglichst viele Daten über eigenes Territorium gehen. Seit den

Anschlägen mit Anthrax-Briefen wird auch die Briefpost überwacht. Auch die Deutsche Post scannt und speichert Absender und Empfänger von Postsendungen.

Man hat bewusst kommerzielle Verschlüsselungslösungen geschwächt. Hersteller von Verschlüsselungssoftware wurden gezwungen, Schwächen in die Verschlüsselung einzubauen. Gute Verschlüsselung funktioniert aber trotzdem. Schwache Verschlüsselung wurde ausgehebelt. Es besteht die Gefahr, dass die gewonnenen Informationen verkauft werden, da zu viele Personen – wie auch Snowden – Zugriff darauf haben. Wie Bruce Schneier sagte: *„What I took away from reading the Snowden documents was that if the NSA wants in to your computer, it's in. Period.“*

Fraglich ist auch, wie sich das Sammeln von Informationen amortisiert. Terrorismusbekämpfung kann alleine nicht reichen. Könnte Boeing auf diese Weise Wettbewerbsvorteile gegen Airbus erhalten haben?

Zu den Auswirkungen der Überwachung zählt, dass vertrauliche Kommunikation kaum mehr möglich ist. Beschädigt werden sowohl Gesellschaft als auch Wirtschaft und langfristig die Demokratie. Grundrechte werden massiv beschnitten und das Vertrauen in Internetdienste ist schwer gestört, was zu massiven Nachteilen für die IT-Wirtschaft (z.B. Cloud) führt. Dies ist aber auch eine Chance für die europäische IT-Wirtschaft, die auf sichere Kommunikation und Privacy by Design setzen kann. Gegen das Abhören, können Gegenmaßnahmen wie Verschlüsselungslösungen oder die Nutzung (kleiner) europäischer Anbieter ergriffen werden. Jedoch gibt es keine Möglichkeit für umfassenden Schutz.

4. Unternehmensverantwortung im praktischen Spannungsfeld

Maximilian Schubert, Generalsekretär ISPA – Internet Service Providers Austria

Der Verband der österreichischen Internetwirtschaft ISPA, dessen Generalsekretär Maximilian Schubert ist, repräsentiert 200 Internetanbieter in Österreich. Mittels der Website www.stopline.at geht sie unter anderem gegen Kinderpornographie und NS-Widerbetätigung im Internet vor, indem einschlägige Vorfälle dort gemeldet werden können. Die Gründung der ISPA geht auf einen Polizeieinsatz zurück. Die Polizei hat Server von Wiener Anbietern abgebaut. Deshalb gab es 1997 einen Protesttag der Internetprovider, an dem es in Österreich „kein Internet gab“.

Schubert behandelte in seinem Vortrag unter anderem die Problematik der Beauskunftung von dynamischen IP-Adressen, dann kam er auf die Umsetzung der Vorratsdatenspeicherung in Österreich zu sprechen. ISPA fordert, dass für die Vorratsdatenspeicherung Richter einbezogen werden: Eine richterliche Bewilligung soll für alle Zugriffe auf Vorratsdaten notwendig sein. Außerdem soll der Staat Daten darüber veröffentlichen, wie viele Zugriffe erfolgen und inwiefern diese Daten im Strafverfahren einen Beitrag zur Aufklärung einer Straftat leisten. Es solle einen Kostenersatz für Internet Service Provider geben, was in Österreich – anders als in den meisten EU Mitgliedstaaten – tatsächlich auch der Fall ist.

Weiters führte Schubert aus, dass die Branche in Zusammenarbeit mit VertreterInnen von Behörden sowie der Zivilgesellschaft das Konzept der Durchlaufstelle (DLS) erarbeitete. Die DLS ermöglicht den einfachen Austausch (CSV-Format) von Informationen und bietet ein Höchstmaß an Sicherheit und Transparenz.

Es besteht eine gute Zusammenarbeit der an der Vorratsdatenspeicherung beteiligten Stellen aber keine ordentliche Statistik. Die Durchlaufstelle hätte diese Statistik nach Vorstellung des Ludwig Boltzmann Instituts für Menschenrechte sicherstellen sollen, leider ist es aber nicht dazu gekommen. Provider sind beträchtlichem Druck ausgesetzt, dabei führen rechtliche Graubereiche zu Problemen. Früher – heute nicht mehr – dachte die Polizei laut darüber nach,

unkooperative Provider als Beitragstätter zu führen. Ein Problem besteht auch, wenn nicht verifizierbar ist, ob eine Anfrage tatsächlich von einer Strafverfolgungsbehörde stammt. Informationen werden daher über eine vordefinierte Kennung erteilt.

5. Völkerrecht: Transnationale IT-Unternehmen zwischen widersprüchlichen rechtlichen Anforderungen diesseits und jenseits des Atlantik

Erich Schweighofer, Leiter Arbeitsgruppe Rechtsinformatik, Abteilung Völkerrecht, Universität Wien

Professor Schweighofer beschäftigte sich in seinem Vortrag mit der Schwierigkeit auf internationaler Ebene einen Konsens zu Fragen des Datenschutzes zu finden. Der Datenschutz ist ein Dissens-Thema zwischen den Staaten, jedoch sind Daten sehr wichtig für die Wirtschaft. Daher müssen transnationale Unternehmen sich mit widersprüchlichen Regeln auseinander setzen. Die Grenzen verschwimmen durch Globalisierung, jedoch bleiben die Staaten wichtige Regulatoren. Die Zivilgesellschaft kann aber mitmischen: Zum Beispiel bei der Internet Governance. Dass Staaten unterschiedlicher Meinung sind, gehört zum Völkerrecht dazu, ist aber problematisch, wenn Daten ausgetauscht werden. Die extritoriale Souveränität ist im Internet sehr stark zu spüren. Daher hat die EU die Verordnung (EG) Nr. 2271/96 des Rates zum Schutz vor extraterritorialen Anwendungen erlassen.

Gegen die von der Europäischen Kommission im Jänner 2012 vorgeschlagene Datenschutzgrundverordnung wird in Brüssel exzessiv lobbyiert, weil effektive Strafen eingeführt werden sollen. In der EU gilt die Verhältnismäßigkeit zwischen Datenverarbeitung und Rechten der Betroffenen sowie die Relativität des Datenschutzes: Zustimmung / Gesetze / Interessabwägung. Dagegen gilt in den USA „reasonable expectations of privacy“, gibt man Daten weg, sind sie weg. Daher ist die USA aus Sicht der EU ein unsicheres Drittland. Es wäre ein weltweiter Kompromiss erforderlich, damit Datenschutz nicht länger Dissens-Thema bleibt. Safe Harbour sollte fürs erste so belassen werden, wie es ist, denn man kommt nicht so einfach heraus. Es fehlt an einer brauchbaren Alternative. Die Compliance-Kontrollen müssen aber zunehmen.

6. Informationssicherheit bei der Telekom Austria Group

Wolfgang Schwabl, Group Director Information Security & Emergency, Telekom Austria

Wolfgang Schwabl beschrieb den konkreten Ablauf von Abhörmaßnahmen in Österreich. Aufgrund einer richterlichen Bewilligung werden diese von der Staatsanwaltschaft angeordnet. Die Polizei führt sie dann durch, indem der Betreiber zur Herausgabe der Daten aufgefordert wird. Die A1 Telekom Austria führt eine rechtliche Prüfung durch, ob die Anordnung rechtmäßig ist, und schaltet sich bei der Vermittlungsstelle (Switches) dazwischen, damit die Polizei zuhören kann. Einen großen Skandal gab es im Juli 2004 bei den Olympischen Spielen in Griechenland. Durch einen Angriff auf Mobilfunk-Switches wurden Anrufe abgehört, indem sie auf Prepaid-Telefone umgeleitet wurden. Aufgefallen ist das erst durch ein Update. Aus Panik wurde allerdings die manipulierte Software gelöscht und so die forensische Ermittlung verunmöglicht.

Im Zusammenhang mit dem Vorwurf gegenüber der so genannten „NSA-Villa“ in Wien wies Schwabl darauf hin, dass es keine Fernverkehrskabel in der Pötzleinsdorfer Straße gebe. Österreichische Medien hatten im Zuge der Snowden-Enthüllungen berichtet, dass in der Wiener Pötzleinsdorfer Straße MitarbeiterInnen der NSA Zugriff auf dort verlaufende Internetkabel hätten und den gesamten Internetverkehr Österreichs „absaugten“. Weiters führte Schwabl aus, dass man Übertragungen von Glasfaserkabeln zwar abgreifen könne, man wisse aber

nicht, was dort durchgeschickt wird. Es sei effektiver die Kabel am Endpunkt abzugreifen. Eine Rechtsgrundlage dafür gebe es nicht.

7. Unter dem Radar der NSA - Überblick über die wichtigsten geheimdienstlichen Methoden und Technologien

Erich Möchel, Journalist ORF.at und IT-Experte

Erich Möchel fasste zunächst die Ereignisse der jüngeren Vergangenheit zusammen. Bei der Belgacom wurde das Datenroaming der EU-Abgeordneten abgegriffen. Die Belgacom habe zwar nicht mitgespielt, sodass man ihr eine „Überwachungssuite untergejubelt“ habe, aber das EU-Parlament gehe extrem fahrlässig mit ihrem Netz um. Die Überwachung funktioniere genau so, wie man es vermutet hatte. Man sei nur über das Ausmaß überrascht. Wie funktioniert sie? Durch einen Splitter werden die Daten in ein anderes Glasfaserkabel kopiert, und zu Switches transferiert, die wie „Mülltrennungsanlagen“ funktionieren.

Die Snowden-Dokumente haben zu einem Schaden für die US-Wirtschaft geführt. Die Aufträge für Cloud-Computing-Reseller seien eingebrochen. Sichere Verschlüsselungsmethoden wie AES seien tatsächlich sicher; die NSA „versaue“ jedoch die Zufallsgeneratoren. Durch manipulierte Zufallszahlen werden elliptische Kurven generiert, die nicht ganz so zufällig sind. Die darauf basierende Verschlüsselung wird somit unsicher, auch wenn die Algorithmen selbst mathematisch sicher sind.

Möchel erwähnte, dass die Hälfte der NSA-MitarbeiterInnen nicht direkt für den Staat, sondern für „Rogue Companies“ arbeiteten und kam dann auf Kryptographie zurück. Die NSA habe diese nicht geknackt sondern ausgehebelt. Die Peripherie und die Implementierung werden angegriffen. Alle Methoden der NSA seien aber „extrem fragil“, weil die erpressten Betreiber mehr Angst vor nationalen Gesetzen hätten als vor der NSA. Natürlich seien die bekannten gewordenen „Hintertüren“ von Belgacom geschlossen worden. Effekte von politischen und technischen Gegenmaßnahmen seien gemeinsam stärker. Die NSA-Systeme werden komplexer aber auch teurer bei sinkender Effizienz.

Zum Abschluss forderte Möchel noch dazu auf, der NSA die Arbeit möglichst zu erschweren. Er riet vom Nutzen von US-Clouds ab. Man solle sein Profil verschleiern indem man verschiedene Browser nützt. Etwas weniger Bequemlichkeit verringere Gefahren auch gegen gewöhnliche Kriminelle.

8. Industriespionage in der Public Cloud: Gefährden PRISM & Co auch die Geschäftsgeheimnisse europäischer Unternehmen?

Gert R. Polli, ehemaliger Leiter des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung (BVT), Unternehmensberater, CEO polli GmbH - Intelligence & Public Safety.

Polli leitete seinen Vortrag mit der Frage ein, ob angesichts der jüngsten Erfahrungen rund um die Snowden Affäre es nicht an der Zeit wäre, eine einschlägige europäische IT-Infrastruktur aufzubauen. Der Spionageskandal und seine Begleiterscheinungen seien eine unglaubliche Chance für die europäische Industrie und einschlägige Unternehmen.

Zum Thema Industriespionage brachte Polli ein sehr beeindruckendes Beispiel aus dem Fundus der Affäre Snowden. Das wirklich erstaunliche heutzutage ist, dass diese ehemals geheimen Informationen heute von der Weltpresse aufgegriffen und auch offen diskutiert werden.

Eines der eindrucksvollsten öffentlich gemachten Fälle zum Thema Wirtschafts- und Industriespionage wurde von einer namhaften deutschen Zeitung im Detail dargestellt. Durch Wikileaks wurden Analysen über den Vertrieb von Hochtechnologie durch deutsche Firmen in

demokratiepolitisch kritische Staaten bekannt. Diese Analyse aus der Feder der NSA zeigt sehr deutlich, wie stark – in diesem Falle – deutsche Unternehmen im Fokus der U.S. Interessenslage stehen. Polli stellte dar, wie intensiv die Aufklärung sein muss, um diese Qualität der Analyse letztlich auf den Tisch zu legen. Die angewandten Aufklärungsmethoden inkludieren Reisedaten, Kreditkartenabrechnungen, Flugbuchungen und selbst die Identifizierung der Dienstreisenden der Firmen. Diese und viele andere Beispiele belegen das hohe Interesse der NSA an Industrie und Wirtschaftsdaten. Der Wert solcher Informationen ist nicht nur ein politischer, sondern auch eine willkommene Basis für außereuropäische Mitbewerber.

Polli nimmt auch Bezug auf den Paradigmenwechsel innerhalb der Nachrichtendienste/Geheimdienste nach 9/11. Bis 9/11 hätten alle Nachrichtendienste eher defensiv agiert. Seither versuchen die Nachrichtendienste, mit allen zur Verfügung stehenden Mitteln Informationen zu sammeln und diese in unterschiedlichen Anwendungen im Sinne des jeweiligen nationalen Interesses auch einzusetzen. Ein zentrales Interesse war und ist der Finanzsektor und hier insbesondere die Kontrolle der weltweiten Finanzflüsse. Insbesondere von den U.S.-Diensten ist ein hohes Interesse evident, die weltweiten Finanzströme zu kontrollieren, und zwar nicht ausschließlich aufgrund des Themas Terrorismusfinanzierung. Polli ging auch auf die Arbeitsaufteilung zwischen NSA und CIA ein. Die NSA sammle Informationen, die CIA setze diese Informationen im Sinne der jeweiligen nationalen Zielsetzung um. Als Beispiel nennt Polli die unmittelbare Einflussnahme der Dienste auf die Bankenlandschaft. Dies wirft auch ein Schlaglicht auf das Thema Bankgeheimnis.

Polli zum Thema Terrorgefahr und Terrorismusbekämpfung: Mit dem Argument der Terrorismusbekämpfung wurde in den letzten zehn Jahren die Privatsphäre ausgehöhlt und gesetzliche Rahmenbedingungen geschaffen, die nachweislich nicht der Terrorismusbekämpfung gedient haben.

9. Wie kann und soll die Politik in Österreich und der EU auf die bekannt gewordenen Überwachungsaktivitäten reagieren?

Waltraut Kotschy, ehemaliges geschäftsführendes Mitglied der österreichischen Datenschutzkommission (DSK), selbständige Konsultantin, externe Datenschutzexpertin des Ludwig Boltzmann Institut für Menschenrechte (BIM)

Waltraut Kotschy erläuterte, dass für die Frage nach den politischen Handlungsmöglichkeiten eine Analyse der rechtlichen Handlungsmöglichkeiten wesentlich sei. Zu diesem Zweck müssen die Kompetenzen der EU und jene der Mitgliedstaaten in Bezug auf die betroffene Materie untersucht werden.

Die EU habe keine unmittelbare Kompetenz, gesetzgebende Akte in Reaktion auf die Enthüllungen zu erlassen, da die Kompetenz zur Rechtssetzung im Bereich des Strafrechts und der nationalen Sicherheit den Mitgliedstaaten der Union vorbehalten sind. Andererseits wäre aber eine Reaktion auf Ebene der EU sinnvoll, weil diese viel größere Bedeutung habe als die der einzelnen Mitgliedstaaten. Wieder einmal ist es allerdings der Kompetenztatbestand „Datenschutz“, der eine Rechtsgrundlage für rechtssetzende Maßnahmen der EU liefern könnte. Soweit die EU jedoch bisher von ihrer Zuständigkeit für Regelungen im Bereich „Datenschutz“ gebrauch gemacht hat, habe sie nachrichtendienstliche Tätigkeiten davon ausgenommen. Dies gelte auch für die derzeit laufende Datenschutzreform.

Kotschy erkennt jedoch eine gewisse Parallele zum SWIFT-Fall, bei dem es – freilich in einem wesentlich begrenzteren Fall – ebenfalls darum gegangen sei, dass Datenströme – mit Provenienz aus der EU – zur Verdachtsgewinnung von US-Behörden durchforstet wurden. Diesbezüglich habe die EU auf Grundlage der Datenschutzkompetenz mit den USA eine vertragliche Lösung verhandelt, die eine aus europäischer Sicht völlig untragbare Situation zu-

mindest verbessert habe, auch wenn man über das SWIFT-Abkommen sicherlich nicht vollkommen glücklich sein könne.

Dies zeige, in welche Richtung eine denkmögliche Lösung auch in diesem Fall gehen könnte, weil andere Konsequenzen – wie zum Beispiel strafrechtliche – nicht gangbar seien. Ihr sei natürlich bewusst, dass dies wenig befriedigend sei, stellte Kotschy mit sichtlichem Bedauern abschließend fest.

Den Abschluss der Veranstaltung bildete eine von Christof Tschohl moderierte Podiumsdiskussion der Vortragenden unter umfassender Einbeziehung des Publikums, das sich sehr interessiert zeigte, und die angesprochenen Probleme der Überwachung noch um weitere Aspekte ergänzte. Das OCG Forum Privacy dankt allen SprecherInnen und BesucherInnen für ihr Interesse und die Teilnahme an der Veranstaltung.

INFORMATION POLICY AND CITIZENS' COMMUNICATIONAL RIGHTS AS CONDITIONS FOR SUSTAINABLE FISCAL POLICY IN THE EUROPEAN UNION

Tuomas Pöysti

Auditor General of Finland, President of the National Audit Office of Finland (Supreme Audit Institution and Independent Fiscal Institution of Finland)

Dr. Tuomas Pöysti, Administrative law (University of Helsinki)

tuomas.poysti@helsinki.fi

Key words: *Information Law, European Union Law, Constitutional Law, Information Policy, Communication Policy, Open Data, Open Government, Transparency, Fiscal Policy, Public Finances, Economic and Monetary Union*

Abstract: *The reform of the rules on the economic governance in the European Union's economic and monetary union (EMU) revises the information and communication policy on economic and budgetary matters in the Union Member States. Transparency is seen as a teleological tool of promoting sustainable fiscal policy and to rectify some longstanding core problems of fiscal policy: the expenditure bias, short-term perspective and fiscal illusion. Transparency rules can be attached to the concept of citizens' informational and communication rights. Citizens' informational rights define essential elements of public participation and democratic order. Citizens' informational rights include access to data and information, access to background knowledge including underlying assumptions and even access to software related to background knowledge, right to belonging to a community and right to self-expression, being heard and listened to. The new European Union economic governance rules have the potential to strengthen citizens' access to information and knowledge and hereby deliberative aspects of democracy albeit the Union has also developed towards a strengthened dominance by a transnational network of the executive side of the government at the detriment of democratic legitimacy. Union's information policy in the economic and budgetary matters strives for an enlightened public debate. Such ideal sets very high demands for participants. Right to knowledge with fair view on complex economic matters requires efficient communication of uncertainties and risks rather than the presentation of simple figures and policy recommendations without alternatives. The new EU rules of the economic governance, in particular the EU Budgetary Frameworks Directive 2011/85/EU establishes an obligation to publish and provide right of access to underlying parameters, assumptions and methodologies as part of the access to information rights. Informational rights and information policy in the area of EU economic governance is an example of the developments in a specific field of public policy and law which are of general significance beyond the specific policy-field concerned. This paper aims to contribute to the development of a systematics of citizens' informational rights and a communication strategy of fiscal policy which is founded on the democratic values of participation, right to know and enlightened public debate.*

1. Introduction and research question

The European Union establishes an economic and monetary union which is an example of the constitutionalisation, the transnationalisation and the supranationalisation of economic and fiscal policies.¹ The economic and monetary union consists of the monetary union, the economic union with the coordination and surveillance of the economic policies of the Union Member States and, lately, since the crisis starting in 2008 an emerging banking union with the single supervision of the credit institutions and the single crises resolution mechanism and the mechanisms for financial stability. The economic union is founded in Art. 121 of the Treaty on the Functioning of the European Union on the coordination of the economic policies and regarding them as a common concern (the preventive arm of the Stability and Growth Pact) and in Art. 126 of and Protocol 12 to the Treaty on the Functioning of the European Union on the avoidance of excessive deficits and reference values to the ratio of public debt to GDP and government deficit (the corrective arm of the Stability and Growth Pact). The economic union is essentially based on the Stability and Growth Pact which is a mixture of binding legal texts of Union law and political commitments. The European Union Stability and Growth Pact is the collection of secondary law of the European Union to implement requirements in the Treaty of the European Union on the budgetary surveillance of the Member States. The Stability and Growth Pact consists of a preventive and a corrective arm, the first aiming to keep budgetary positions within the sustainable path and within the reference values and the latter aiming to rectify excessive government deficits or debt.²

Since the financial crisis started in 2008 and the euro area debt crisis unfolded on this occasion, the legal framework of the Economic Union and the Stability and Growth Pact has been complemented by new legal provisions in which the so-called Six Pack and Two Pack reforms have been among the most significant changes (respectively in 2011 and 2013).³ The enforcement of the preventive arm was strengthened with the adoption of the Regulation (EU) No 1173/2011 of the European Parliament and of the Council of 16 November 2011 on the effective enforcement of budgetary surveillance in the euro area, which together with Council Regulation (EC) No 1466/97 forms the preventive part of the Stability and Growth Pact. The corrective arm of the Stability and Growth Pact has been further strengthened by one of the so called Two Pack regulations, the Regulation (EU) No 472/2013 of the European Parliament and of the Council of 21 May 2013 on the strengthening of economic and budgetary surveillance of Member States in the euro area experiencing or threatened with serious difficulties with respect to their financial stability. As the name indicates this Regulation concerns Euro area countries with serious economic difficulties and establishes specific steering processes for them. Another piece of the Two Pack regulations, Regulation (EU) No 473/2013 of the European Parliament and of the Council of 21 May 2013 on common provisions for monitoring and assessing draft budgetary plans and ensuring the correction of excessive deficit of the Member States in the euro area,⁴ hereinafter the Draft Budgetary Plans

¹ Habermas 2012a.

² A good general presentation of the Stability and Growth Pact is European Commission 2013a. A more technical and detailed guide targeted to expert audiences and which also informs the way in which the European Commission interprets the calculation of the key reference indicators is European Commission 2013b.

³ Terms Six Pack and Two Pack refer to the European Commission proposals to strengthen the Stability and Growth Pact and the Economic Union. The Six Pack consisted of 6 legislative acts of the Union, the Commission presented its legislative proposals in 2010 and the Six Pack consisting of six legal acts became law in 2011. These legal acts were complemented by the Two Pack in which two new Union legislative acts became law in 2013. For a general introduction see http://ec.europa.eu/economy_finance/economic_governance/index_en.htm (page visited 21.12.2013).

⁴ Regulation (EU) No 473/2013 of the European Parliament and of the Council of 21 May 2013 on common provisions for monitoring and assessing draft budgetary plans and ensuring the correction of excessive deficit of the Member States in the euro area, OJ L 140, 27.5.2013, p. 11–23.

Monitoring Regulation, applies to all Euro area countries, and seeks to embed European policy guidance and European rules to the national budgetary procedures and public debate.

The European Union economic and fiscal governance framework extends beyond the Stability and Growth Pact. The Stability and Growth Pact is complemented by Council Directive 2011/85/EU of 8 November 2011 on requirements for budgetary frameworks of the Member States, hereinafter the Budgetary Framework Directive.⁵ The Budgetary Frameworks Directive has a potentially significant impact on the national fiscal governance and communication and information policy related to economic affairs. Together with Regulation (EU) No 473/2013, the Budgetary Framework Directive establishes a new national dimension of the information and communication policy related to the coordination of economic and fiscal policies in the European Union.⁶

The legal framework of the Union law is complemented by the provisions of public international law. Twenty-five Member States of the European Union have signed the Treaty on Stability, Coordination and Governance in the Economic and Monetary Union (TSCG) which contains a Fiscal Compact reinforcing and complementing the Stability and Growth Pact in the national law of the Member States. With economic governance, reference is made to all legal instruments and rules concerning coordination of economic policies and in particular budgetary policies of the European Union Member States.⁷

A strengthened European economic union and the coordination of economic and budgetary policies within it also creates a specific information policy and communication policy applied to the economic and budgetary matters. The Fiscal Compact and Six Pack and Two Pack acts of the Union require, among other things, the establishment of independent fiscal institutions as producers and disseminators of independent information and assessments of economic policies and macro-economic and budgetary forecasts. The independent oversight bodies, Independent Fiscal Institutions, often also referred to as fiscal councils, are established in order to improve the quality of information and to be active participants in the public debate.⁸

Information policy is comprised of laws, regulations, doctrinal positions and practises with society wide effects concerning information creation, processing, flows, access and use.⁹ It defines rules and policies concerning access to governmental information and use of governmental information resources. Communication policy can be defined in similar terms as rules, policies and practises concerning communication(s). Information policy itself is very closely related to the constitution

⁵ Council Directive 2011/85/EU of 8 November 2011 on requirements for budgetary frameworks of the Member States, OJ L 306, 23.11.2011, p. 41–47.

⁶ Albeit in the context of the economic union the Treaty on the Functioning of the European Union speaks about economic policy, the core of the Economic Union concerns public finances of the Member States and, thus, fiscal policy. Fiscal policy can be shortly defined as the measures in which the government seeks to impact society and national economy by making decisions concerning the level and general structure of the public sector revenue and expenditures (public finances), National Audit Office of Finland, *Finanssipolitiikan tarkastusohje* (Instructions on Fiscal Policy Auditing), valtiontalouden tarkastusvirasto 2011, p. 7.

⁷ For a general description of the economic governance in the Euro Area and the European Union, see the European Commission Press Release 12 November 2013, European Commission - MEMO/13/979 12/11/2013, EU's economic governance explained, http://europa.eu/rapid/press-release_MEMO-13-979_en.htm?locale=en (page visited 21.12.2013).

⁸ In Finland the National Audit Office of Finland is, in addition to its constitutional role as Supreme Audit Institution, also the Independent Fiscal Institution, pursuant to section 1 of the Act on the National Audit Office of Finland (Act 676/2000) and the Fiscal Policy Act (Act 869/2012).

⁹ Definition is from Braman 2011, p. 3. Here I have dropped from professor Braman's definition terms practises with constitute effects, since, for a constitutional lawyer, something characterised as constitutive attaches a specific value and higher status.

and law.¹⁰ The foundations for information and communication policy are set in constitutional texts or practises of constitutional character.¹¹

Economic and fiscal policies are a core area of democracy and of the public sphere. Fiscal policy can also be considered a super-policy among governmental policies since decisions in the field of fiscal policy define resources and possibilities within which the government can exercise its functions, promote its policies and guarantee fundamental rights and freedoms.¹² Historically, the roots of parliamentary way of government lie in the right of the citizens' collectively to give consent to taxes to be collected by the sovereign. The evolution of the economic governance and the informational policies and practises related to it are therefore an important field for an even broader analysis of the evolution and the shape of democracy. Recent developments, on the other hand, show risks in the strengthening of the executive and decision-making which is not subject to public debate and transparency.¹³

In this article, I study *which is the information policy and communication policy established by the Budgetary Framework Directive 2011/85/EU and the Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 together with the Treaty on Stability, Coordination and Governance in the economic and monetary union*, hereinafter the TSCG, which contains as one of its chapters the Fiscal Compact. I will consider the evolution of the concept of transparency and citizens informational and communicational rights which can be observed in these laws and treaties on the economic governance.

The specific scientific task in this article is the analysis *which are citizens' informational rights the new provisions in the European Union law concerning transparency of fiscal policy seek to establish and promote*. My aim is to discuss how these new legal provisions *can contribute to the concept of deliberative democracy in the current, contemporary and very internationalised society*. I share my reflections on the extent to which the recognised communicational rights may remedy some of the core economic problems in fiscal policy; fiscal illusion, over-consumption of public services and benefits and the expenditure biases. This piece aims to contribute to the development of a communication strategy of fiscal policy, which is founded on the democratic values of participation and right to know and on the enlightened public debate, but which is also effective in the realisation of the objectives of the revised rules of economic governance in the European Union.

2. Methodological remarks: critical constructivism and constitutional law in the analyses of information policy

This article provides an analysis of information law and information policy. Information law and information policy are by their nature multi-disciplinary. Information law is approached here from the angle of constitutional law. Information and communications studies as well as economics support this insight into information law and constitutional law. However, within the scope of this paper, I will not perform an economic analysis of fiscal policy governance nor of the information policy related to it. Ultimately, this piece is an analysis of theoretical legal dogmatics and jurisprudence giving a legal science contribution to the wider perspectives of information policy.

¹⁰ For example Sandra Braman cites the 21 provisions related to information policy in the U.S. Constitution and Bill of Rights, see Braman 2011, p. 2.

¹¹ Similarly Braman 2011.

¹² Negatively this is seen in the impact of some fiscal policy measures to the fundamental rights and freedoms, see Council of Europe 2013.

¹³ Habermas 2012b is a strong and well-argued warning of the risks.

I will use an approach which can be called critical constructivism. Hence, I will try to strengthen a possible systemic interpretation of the new Union laws and treaty provisions on economic governance and to give a transparency and democracy-friendly interpretation.

My specific purpose is to contribute to the critical discussion on the normative models of democracy in the European Union and, in particular, to highlight which positive potential and challenges for democracy lies in the new legislation and governance arrangements of economic and fiscal policy. My hypothesis here is that some of the provisions in the strengthened fiscal governance have potential to strengthen the deliberative aspects of democracy and improve transparency.

The new fiscal governance arrangements in the European Union and Euro Area have been subject to severe criticism in the public debate, the political debate and in the academia. The Finance Committee of the Parliament of Finland was concerned that, on some occasions, the TSCG imposes significant limitations to the national budgetary powers and therefore, the consequences of the entirety of the small individual changes in the European Union economic governance to the national budgetary powers and democracy should be closely monitored. There was even some unease with the Constitutional Law Committee of the Parliament of Finland, which according to the Constitution of Finland has primacy in the ex-ante examination of the constitutionality of laws, since the Constitutional Law Committee did not see such a strong limitation. The Constitutional Law Committee considered the TSCG Treaty and the new economic governance rules to be more or less acceptable by the the Constitution.¹⁴ The Minister of Foreign Affairs of Finland, Dr. Erkki Tuomioja has repeatedly stated that the management of the European debt crisis has damaged European democracy at least as much as the irresponsible economic management has damaged the sustainability of European public finances. TSCG with the Fiscal Compact was drafted in a non-transparent way in which ordinary legislative and treaty revision procedures were set aside in a process led by Germany and France, not by the EU Institutions.¹⁵

The European Union financial and debt crisis has also a deeper aspect of constitutional crisis. According to some critique, the Union is developing into a direction of a control union or discipline union in which democratic decision-making is replaced by technocratic control by non-elected officials.¹⁶ Financial and debt crisis has created challenges and changes to the democratic legitimacy and accountability. To make this situation more complex, the economic policy coordination has in the Treaties on the European Union all the time been subject to different rules than the majority of the Union action and hereby general rules of the Union law and of the functioning of In-

¹⁴ See the Report of the Finance Committee of the Parliament of Finland on the ratification of the TSCG, VaVM 38/2012 vp. and the Opinion of the Constitutional Law Committee of the Parliament of Finland, PeVL 37/2012 vp. The author of this article contributed as expert to the Committee deliberations on both Committees. The Finance Committee heard the chairman of the Constitutional Law Committee in expert hearing as an expert, which is a very uncommon procedure in the Parliament of Finland where Constitutional Law Committee Opinions usually are taken as authoritative and are not challenged. Criticism towards too flexible constitutional analyses in the face of an eventual limitation of national parliamentary budgetary powers is also presented by some well-known economists. Raimo Sailas, the former permanent state secretary of the Finnish Ministry of Finance, considers new Treaty and legislative acts on economic governance as a significant limitation of the national budgetary powers and thereby leading to severe deepening of the democratic deficit of the European Union, see Sailas 2013.

¹⁵ See the comments by the Minister of Foreign Affairs of Finland, Dr. Erkki Tuomioja in Talouselämä 46/2012.

¹⁶ See, among others, Habermas 2012a and 2012b. In Finland a well-known constitutional lawyer, professor of the Academy of Finland Kaarlo Tuori has repeatedly raised his voice to the problem of legitimacy in the crisis decisions and development of European Union towards a technocratic control union. This risk of control union or discipline union and the lack of legitimacy is also taken up in the National Audit Office of Finland Special Parliamentary Report on the audit of the central government financial statements and Government Report on Final Accounts of year 2011, NAOF Parliamentary Report K 14/2012 vp., valtionalouden tarkastusvirasto 2012. A good academic critical reading of the euro area crisis combining constitutional law and economics is Tuori & Tuori 2014.

stitutions is not applicable. Economic policy is an exceptional area of Union policies and subject to higher degree of inter-governmentalism than other areas of Union policies.¹⁷

Some economists have criticised new provisions of economic governance as a set of confusing and overlapping rules which are subject to many discretionary elements and, hence, subject to a multiplicity of interpretations. The new Fiscal Compact and the rules of the Stability and Growth Pact since the reform of 2005 define a rule on the structural balance of general government. The problem, according to critics, is said to be that the calculation of the structural balance is complicated and requires a series of discretionary analyses and estimates. There is no genuine agreement among the community of economists on the computation of the structural balance and, in particular, the estimation of potential GDP, which is required as a step in the computation of structural balance.¹⁸ Despite this technical character the rule expressed in terms of structural balance sets the limits for political discretion on budgetary matters. Power then deludes to non-transparent exercise by the experts. This example of the mathematisation is one of the phenomena present in today's information policy.¹⁹

Revised rules on economic governance in the Euro Area and the European Union are multi-faceted and contain different governmentalities, or, at least potentials for different governmentalities. Governmentality here is a foucaultian term referring to the cultural and epistemic patterns out of which governance and government arise and by which they are produced and maintained.²⁰ Government means formal administration co-ordination processes, laws and organisations whereas governance means both formal and informal rules, practises and decision-making processes to steer activities and influence behaviour, risks and organisational structures.²¹ Governance extends beyond the role of the traditional nation-state government to cover also co-ordination and steering activities of private actors and supra- and transnational actors. Despite criticisms, the new European Union fiscal policy governance rules contain also several elements of increased transparency and improved participation and elements of deliberative democracy. My intention is to trace these elements of governmentality and strengthen their visibility and bring them to a more central stage in the systematisation and systemic legal reading of the rules. Thereby I aim to strengthen the participatory legitimacy and deliberative democracy in the system of the economic governance of the European Union.

My approach is influenced by the realism and critical legal studies. But rather than simply telling a critical narrative of what is wrong, I try to construct an alternative system which deliberately strengthens features and governmentabilities which are present, but not necessarily yet in a dominant position.²² I observe the potentials for strengthening deliberative aspects of democracy in the new EU fiscal policy governance system. By doing so, I will also actively counter-balance the tendencies to less transparency and increased technocratic control.

¹⁷ Leino-Sandberg & Salminen 2013.

¹⁸ In Finnish context see Ilmakunnas 2012. Criticism from the economic perspective unnecessary complexity of the rules which brings with risks to legitimacy presented by the OECD economists see OECD/Barnes, Davisson and Rawdanowich 2012, which contains also an analyses of the likely impacts of the new fiscal rules in Europe. On the technical computation of structural balance, see valtionalouden tarkastusvirasto 2013c.

¹⁹ Braman 2006, p. 316 – 317.

²⁰ My definition here follows the definition by professor Braman, see Braman 2008. I have however added emphasis on the knowledges and structures of knowledge as essential features of governmentality.

²¹ Braman 2008, 433.

²² My approach is inspired by Kaarlo Tuori's critical assessment of the Crits approach to law and aims to take into consideration the double identity of legal scholarship as participant in the academic debate but also as an actor of the legal system shaping and modifying the legal system itself, see Tuori 2007.

3. Citizens' communicational rights in constitutional democracy

3.1. Citizens communicational rights in the constitutional order and information policy

Citizens' informational and communicational rights are an important topic in law, media studies and politics. Law establishes the informational and communicational constitution of society. Law also reproduces and communicates the fundamental principles and conventions at the level of social contract on conditions and framework of communication, and hence, provides foundations for legitimacy. Certain of these principles are old and relate to the position of individual in social relations and in relations to authorities in different formats. Some of these principles and conceptions are new and in the process of change following fundamental changes in technology, societal and economic conditions and in the conception of democracy. Constitutional foundations for legitimacy are dynamic and take place in communicative actions.²³ Informational and communicational rights are principles at the level of the social contract and conventions. They have their foundations in the texts of Constitutions and at the European Union in the European Charter of Fundamental Rights, case law of the European Court of Justice and the European Court of Human Rights and in the constitutional traditions of the Member States. Their expressions are results of objectivation by legal studies and constitutional practises.

Citizens' informational and communicational rights define fundamental aspects of the conditions of participation to markets and to social and public life. Citizens' informational and communicational rights also determine public sphere as part of the overall arrangements of democratic governance and rule of law. The public sphere is a distinct set of social relations in which information and discussion is as default shared with other members of the polity and in which the members also recognise the distinct common public interest. The informational and communicational rights and the emphasis set on them individually vary to certain degree depending on the specific form of democracy and democratic legitimacy chosen in a particular democratic polity, a political community based on the horizontal association of free and equal legal persons, a bureaucratic organization for collective action, and civic solidarity as a medium of political integration.²⁴ Informational and communicational rights also define foundations of the information policy in each political system.

Professor Hannu Nieminen has from the perspective of media studies recognised principles which crystallize citizens' communicational rights. Nieminen's definition develops further on earlier discussions and practical guidance on international arenas.²⁵ Definition of communicational rights, or rather, principles, can be used to analyse media and its regulation and, to provide a systematic framework for the analysis of law and media practises. These principles also provide a normative tool to analyse and develop recommendations concerning communication and information policies of the government. From the information law viewpoint, these rights represent meta-rights or general principles of information law.²⁶ Citizens' communicational rights according to professor Nieminen are (1) right to factual information, (2) right to background information and knowledge, (3) right to a belonging to a community including a right to entertainment and (4) right to self-expression. These rights or principles aim to connect the idea of informed citizenship with the communicational rights and regulation and steering of communication.²⁷

²³ This is an interesting point by Habermas 2001. The performative action bringing legitimacy is renewed all the time and is not a static historical fact or a fiction situated on ancient times.

²⁴ Definition of democratic polity is borrowed from Habermas 2012a, p. 339.

²⁵ See, for example <http://www.crisinfo.org/>, page visited 1.7.2013.

²⁶ Pöysti 2004 and Pöysti 2002.

²⁷ See Nieminen 2007.

(1) *Right to information and knowledge (factual information)*. This dimension concerns access to brute facts and data. Right to information or, access-to-information is provided by the freedom of information laws, in the European Union law the foundations being Article 42 of the Charter of the Fundamental Rights and Article 15 of the Treaty on the Functioning of the European Union and Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents.²⁸ These norms of the Union law concern the Institutions and bodies of the Union. They do not regulate the access-to-information in the governments of the Member States of the Union. The legal situation on the access-to-government information is scattered and fairly different in the various Member States.²⁹ Some specific acts of the Union have, however, regulated access to information in the Member States, environmental information having been the first area to be covered by a European access right already in 1990.³⁰ Access to facts, data and background information making data usable and understandable in the budgetary process and economic policy area is now (partly) covered by provisions in the Budgetary Frameworks Directive 2011/85/EU. The Directive establishes information policy and information right with regards to the data and information on the Member States governments. On the access to data in the context of the economic and fiscal policy, the statistical regulations of the Union additionally define core principles of the information policy, in particular concerning statistical principles and access-to confidential background data underlying statistics.³¹

(2) *Right to background knowledge* concerning social and political choices, that is the right to best possible reasonable knowledge on the topic on public agenda and on the consequences of the various alternative decisions. This dimension concerns the right to factual orientation to analyse and understand the context and significance of factual information and societal policies. In other words, this right can also be called right to contextualised understanding or *access to contextualised knowledge*, where the objective is to create understanding beyond the mere reporting of single documents and brute facts. Union law is increasingly interested about the material conditions for the creation and attainment of such knowledge. European policy initiatives on the open access to scientific data and information create conditions for further use and cumulation of scientific data

²⁸ Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30th May 2001 regarding public access to European Parliament, Council and Commission documents, OJ L 145, 31.5.2001, p. 43–48. European Commission has in 2008 tabled a proposal to replace the current Regulation with a new regulation, see COM (2008) 229 final – 2008/0090/COD. Commission amended its proposal in 2011, see COM (2011) 137 final. European Parliament adopted EP Opinion in the 1st reading on 15.12.2011. European Parliament amendments highlighted the role of transparency and access to documents and information to the endeavours for better regulation and to the functioning of democracy. Purpose in the reform of Regulation (EC) No 1049/2001 is mainly to codify in the Regulation changes following from the entry into force of the Lisbon Treaty and the case law of the European Court of Justice and European Court on Human Rights.

²⁹ A good comparative analyses of the freedom of information laws in Finland, Germany and in the federal law of the United States is Bräutigam 2008.

³⁰ Currently Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, OJ L 41, 14.2.2003, p. 26–32. Access rights to environmental information were already created by the Council Directive 90/313/EEC. The Council Directive 90/313/EEC was very modern at the time, it also specifically addressed the issue of information held in databases seeking to guarantee to any natural or legal person throughout the Community free access to available information on the environment in written, visual, aural or data-base form held by public authorities, concerning the state of the environment, activities or measures adversely affecting, or likely so to affect the environment, and those designed to protect it.

³¹ Regulation (EC) No 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC, Euratom) No 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities, OJ L 87, 31.3.2009, p. 164–173.

and making knowledge easier available.³² In the economic governance, the establishment of Independent Fiscal Institutions as independent oversight bodies and participants to discourses on economic and budgetary forecasting and on fiscal policy preparation and assessment in accordance with the common principles on the automatic correction mechanism in the Fiscal Compact, Budgetary Frameworks Directive and Regulation (EU) No 473/2013 can also be seen in the light of strengthening the contextualised background knowledge.

Several access-to-information laws (freedom of information laws) include the right to background knowledge as a legal principle or a policy goal of legislation. In Sweden, in the 1970s already, the Swedish publicity legislation was pursued a legislative goal – in Ronald Dworkin’s terms legal policy – that public authorities shall produce and distribute information on societal conditions and this information then can be basis for journalism, citizen participation and analyses by researchers. In Finland, this legal policy has then been included into section 19 of the Openness in the Government Act (Act 621/1999).³³ Active production of information by public authorities and giving conditions for public debate is also found in Finnish law in section 29 of the Act on local government (Municipalities act, Act 365/1995).³⁴ The Budgetary Framework Directive 2011/85/EU Article 4 sets the requirement to make available assumptions, parameters and methodologies which have been used in macro-economic and budgetary forecasting and also an obligation to the Member States governments to produce and make publicly available comparative analyses of the macro-economic forecasts and sensitivity analyses on alternative scenarios. In addition, the Member States have according to Article 3 a duty to make publicly available timely information on the financial situation of all the subsectors of the general government including monthly and quarterly reporting. Obligations under Article 3 mean obligation to produce cash-flow statements regularly and also to make available meta-data on the content of the information. Even in a Member State with fairly sophisticated public sector financial management and reporting systems, the implementation of Article 3 of the Budgetary Framework Directive require additional action.³⁵

The Treaty on the European Union and the Treaty on the Functioning of the European Union, the two Treaties on which the European Union is founded, set a strong emphasis on openness, dialogue and transparency as a statement of values and political and legal principles the Union itself and also its Member States adhere to.³⁶ Openness and transparency principles can be read to include the right to background information and contextualised knowledge. Very specific area of this kind of background information are the regulatory impact assessments concerning which the general policy of the Union is expressed in the several policy documents on better regulation and on which the OECD has produced recommendations and documents which represent the common understanding of policy-drafting and policy ideals in Western countries. The European Parliament underlined several aspects of the openness and the need to improve quality and openness of impact assessments and policy-analyses in its opinion on the 1st reading of the recasting of the Union’s Transparency Regulation 1049/2001.³⁷ Albeit according to preamble and legislative history, the

³² See European Commission Proposal for the amendment of the Re-use of the Public Sector Information Directive, the PSI-Directive, COM (2011) 877 final, p. 5.

³³ Pöysti 2007.

³⁴ Mäenpää 2013, Chapter IV.3, p. 615-616.

³⁵ See on the measures needed in Finland, the Finnish Ministry of Finance Working Group Memorandum on the national implementation of the Budgetary Framework Directive and Draft Budgetary Plans Monitoring Regulation, valtiovarainministeriö 2013.

³⁶ See Articles 1 and 9 -12 of the Treaty on the European Union and Article 15 of the Treaty on the Functioning of the European Union.

³⁷ European Parliament Opinion on the 1st Reading, P6_TA(2009)0114, OJ C87, E362, 1.4.2010. See the European Parliament Rapporteur’s Report: Report on the proposal for a regulation of the European Parliament and of the Council regarding public access to European Parliament, Council and Commission documents (recast),(2008/0090(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Michael Cashman,

Budgetary Framework Directive seeks primarily to improve the quality of macro-economic forecasting and rectify the risks of over-optimistic economic forecasts and forecasting errors, the development of the access-to-background information and production of comparative information can be seen as part of a wider trend towards production of policy assessments and making them available as part of the idea of open government.

(3) *Right to a belonging to a community* which also entails a right to entertainment and arts and a right to inter-action via media. In this dimension, media and communication are forums of participation and social engagement. Right to a community includes both private and public spheres, which are increasingly blurred on certain areas but which ultimately have very distinct legal characteristics. Here, I will focus only on the public and the political dimension of the right albeit in the communication's regulation the private aspects including the media and entertainment are very significant. Right to a belonging to a community is ultimately a political right and refers to the rights of participation in a political community. Media and debates in media produce also the community as a forum of civic and political solidarity and arena for discussing and solving political issues.³⁸ Production and distribution of information provisions in the freedom of information laws aim also at the strengthening of the participation to public life in the political community.³⁹ Improved knowledge also is said to strengthen trust to the institutions of a political community, which is one of the functions of the publicity principle and access-to-government documents and information.⁴⁰ Debates of the economic and fiscal policy are at heart of the concept of political community since it is about the issue how common resources and public capacity to influence economic structures for the welfare of the community and for the common good shall be exercised. The purpose of the new economic governance rules, in particular the Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 and the Budgetary Framework Directive 2011/85/EU, is to strengthen public debate and knowledge in the Member States about the sustainable and disciplined fiscal policy and to integrate the European Commission analyses on macro-economic forecasting to the national political debates. The new economic governance rules clearly admit that the Member States are an important polity – political community – in the European Union. They represent a double strategy in trying to develop the Union itself as a political community, of which the role of the European Commission and, in particular the role of the European Parliament, are examples of, but also to develop the public discourses on disciplined fiscal policy in the Member States political communities.

(4) *Right to self-expression* which does not only cover the formal freedom of expression but a right to become heard and taken into account in communications, simply being listened to. Ultimately the question is about the right to enjoy respect and feeling of being taken into account. Often forgotten dimension is also *the right to be listened to* and listening: most models of deliberative democracy and deliberation put in advance active discussion and are silent about listening.⁴¹ Right to self-expression via media is guaranteed by Article 11 of the European Union Charter of Fundamental Rights and it is in the core of the fundamental right to freedom of expression as it has been

EP A6/2009/77. The Commission presented in 2011 another amendment to the Transparency Regulation but the various procedures have been merged under procedure 2008/90/COD. The European Parliament has adopted its opinion 15.12.2011, see P7_TA(2011)0580 (2013/C 168 E/45), OJ C 168/E159 14.6.2013.

³⁸ The problem of the new European economic governance is exactly that neither the governments nor the media support the addressing European problems in the national media and political arenas, see Habermas 2012b and 2012a. Habermas, however, has a very optimistic opinion, and too idealistic view of the possibilities of traditional media to perform such role in the new fragmented and international environment.

³⁹ From the perspective of Finnish law, see Mäenpää 2013, chapter IV.3.

⁴⁰ See, for example the European Parliament's 1st Reading Opinion on the recasting of the Union's Transparency Regulation (EC) N0 1049/2001, P7_TA(2011)0580 (2013/C 168 E/45), OJ C 168/E159 14.6.2013, COD 2008/90.

⁴¹ See Dobson 2012.

developed in the case law of the European Court of Human Rights. The right to be listened to becomes close to the right of participation and right of being heard which are significant elements of the right to good administration protected in Article 41 of the European Union Charter of Fundamental Rights.

The new economic governance rules do not in particular develop the conditions for the exercise of the political communicational rights and rights of participation but nevertheless aim to guarantee the right to self-expression of certain institutional actors. The Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 and the Common principles on the Automatic Correction Mechanism of the Fiscal Compact stipulate that Independent Fiscal Policy Institutions shall have access to public communications. In addition, Two Pack Regulation on the Enhanced Surveillance of the Euro Area Member States with Serious Difficulties (EU) No 472/2013 creates some specific features of dialogue between the Parliament of the Member State concerned and the European Parliament and an involvement of the social partners and civil society.⁴² But apart from this there is hardly anything in the new economic governance rules to strengthen the citizens' right of self-expression and right of participation and being listened to.

This is a challenge since the technical nature of the information on European economic governance may alienate citizens' and the absence of the specific mechanisms of participation and policy alternatives may give a feeling of alienation. Economic and fiscal policies are also at the core of governmental politics and may therefore be subject to mediatisation and spin-doctoring further limiting the possibilities for truly participative political debate. The transition in economy towards an information economy and away from hard empiricism towards representations – images and understanding which are important for economic decision-making, further create a specific challenge to participate in dialogues as legal and policy ideals.⁴³ Tendencies towards spin-doctoring and increasingly representational characters in economy and politics may also lead to limitations to the possibilities of the governmental experts to participate in the public policy discussion albeit, for example under Finnish law, the civil servants have a fairly strong protection for their freedom of expression. On the other hand the aim of improving the general quality of discourses and information in the economic and fiscal policy debates also creates conditions to the right of self-expression and participation.

The point of departure in professor Nieminen's classification of citizens' communicational rights is the idea of informed citizenship. Informed citizenship is one of the preconditions for informed public debate and knowledge-based policy-making. Informed citizenship is a necessary element for a well-functioning democracy, effective democracy (*effektiv folkstyre* in Swedish) in which democracy does not mean only formal free elections and majoritarian rule but the prevailing of circumstances in which the people can truly and effectively participate and influence public decision-making. Informed citizenship is a historical legal ideal in the Scandinavian tradition and one of the founding principles in the Swedish principle of publicity introduced in the early 18th Century by a Finnish representative in the Swedish Diet, Anders Chydenius. In today's law, one of the most beautiful formulations of this idea and the role of the information policy in achieving it are to be found in Article 100 of the Constitution of Norway on the principle of publicity and the role of the public authorities to create foundations for an enlightened public debate and governance based

⁴² See Article 7 (10) and Article 8 of the Regulation (EU) No 472/2013 of the European Parliament and of the Council of 21 May 2013 on the strengthening of economic and budgetary surveillance of Member States in the euro area experiencing or threatened with serious difficulties with respect to their financial stability, OJ L 140, p. 1, 27.5.2013.

⁴³ On the impact of the representational nature of economy to formulation of global information policy, see Braman 2011b.

on such public debate. More analytical explanations of this ideal are found in the Swedish government official documents concerning analyses and changes of principle of publicity in Sweden.⁴⁴

Professor Nieminen's approach to citizens' communicational rights is useful in order to analyse economic governance information and communication policy rules according to the concepts of open government data and re-use of public sector information in accordance with the European Union Re-use of the Public Sector Information Directive 2013/37 /EU.⁴⁵ From a classic public law and access to information perspective, the classification of access rights would start from access to documents and nowadays right of access to a structured data including access to raw data, meta-data and structured information based on them and move on to various legally informed communication policies in accordance with publicity laws and legally created duties for public authorities to produce various materials and make them available in public arena.⁴⁶ Nevertheless, professor Nieminen's classification of communicational rights provides a framework to a well-functioning systematics, and, to normative assessments, critique and development of communication policy in accordance with rules and underlying democratic ideals.

The right to background knowledge has with the Budgetary Frameworks Directive 2011/85/EU and the Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 been expanded in an interesting way to cover also right of access to background assumptions and software applications needed to test reliability and sensitivity of the information. The case of the software and applications is not evident in the text of the Directive and Regulation themselves but in practise where the European Commission makes publicly available the applications it uses for the calculation of the structural deficit. Making the applications available are part of making public the assumptions, parameters and methodologies of analyses required by the Budgetary Framework Directive.

Enlightened governance entails the idea of knowledge-based policy making which can also be traced as one of the ideals in the new European Union legislation on the governance of fiscal policies and in the Fiscal Compact. The knowledge-based policy making itself is a very difficult and troubled political ideal for several reasons. In Finland the knowledge-based policy-making has been strongly advocated in the government and public management reform agendas.⁴⁷ Knowledge-based policy making is a strongly present ideal in the Finnish instructions on the legislative drafting.⁴⁸ This development idealism has not specifically addressed the serious question marks on the possibilities and limits of the knowledge-based policy making in governmental practise and also somewhat ignored the theoretical and practical background assumptions which are necessary for a successful implementation of knowledge-based policy making.⁴⁹

⁴⁴ Pöysti 2007.

⁴⁵ 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, OJ L 175, 27.6.2013, p. 1–8.

⁴⁶ Pöysti 2007 and Pöysti 2004.

⁴⁷ See for example the Prime Minister's Office of Finland publications in which knowledge-based policy making has advanced as one of the core themes of management and governance reform, Valtioneuvoston kanslia 7/2011 and Valtioneuvoston kanslia 8/2011. The strengthening of the knowledge-based decision-making and the evidence-basis of governmental policy-preparation is also one of the lead objectives of the reform of the governmental research institutions decided by the Government in Government Decision on the Reform of the Governmental Research Institutes and Research Funding, done on 5.9.2013, see Valtioneuvosto 2013.

⁴⁸ See Finnish government instructions on law-drafting and on the impact assessment, and in particular the process model instructions of law-drafting approved by the Government and to which the Government has committed itself to, at the legislative data base Finlex, Oikeusministeriö: säädösvalmistelun prosessimalli, <http://lainvalmistelu.finlex.fi/> (page visited 3.12.2013), which contains links to the law-drafting and impact assessment instructions.

⁴⁹ One way to look into the limits of the knowledge-based policy-making is to systematically analyse information flows in the public policy-making and analyse the information processing qualities and quality of information, er-

Not surprisingly, in practise the implementation of it has proven to be very challenging. According to empiric analyses by the National Audit Office of Finland, it is exactly the practical implementation of the knowledge-based decision-making supported with ICT which out of all the topics of suggested management and policy-improvement has been the slowest and most difficult for the government and government entities to implement. Recommendations to improve the knowledge and information base of decision-making and ICT had the least success out of a wide variety of categories of recommendations for public management development. The basic distinction between value rationality and purpose rationality has sometimes been ignored. Consequently, there has not been room for politics and political judgment. The values and political conceptions also influence on human cognition and our ability to use information.⁵⁰ In Finland, the general societal and governmental pragmatism, generally high education level in society and the high valuation of rationality and the principle of publicity, all make the knowledge-based policy-making a highly esteemed ideal which is not easy to question. This valuation and relative success in transparency and pragmatic, rational government and governance system may also create cognitive blind-spots in public management and governance development. The challenges at the background are not then easily recognised.⁵¹

Professor Nieminen's mapping of the citizens' communicational rights comes very close to my legal systematisation of the principles of information law as a distinct body and discipline of law. The general principles of information law are (1) right to information and freedom of information entailing access to data and documents, access to information, right to use information and the free flow of information; (2) right to communication and freedom of communication; (3) the right to knowledge and freedom of knowledge; (4) the right to public and private self-determination; (5) the right to privacy; (6) the right to efficiency in the markets and in public administration; (7) the right to information security; and (8) the right to quality and good governance.⁵² Both the rights to information and communication are multi-dimensional rights and ideals. Nieminen's analysis captures also the significance of entertainment and arts from a participatory and democratic perspective which is often forgotten in legal analyses. Entertainment is not at the core of the analyses of the governance of fiscal policy but may not be forgotten. A general trend in the media is the focus on human interest and narrative approach of appealing or exciting stories and dramas. Politics and policy are in the process of becoming increasingly mediatised and elements of entertainment sweep into it. Economic news and politics themselves are also a kind of entertainment in the contemporary media society. The essential point is that professor Nieminen uses the citizens' communicational rights to analyse and develop practises of media. Similarly the communicational rights and the principles of information law can be used to develop systematic and democracy-friendly interpretation of new EU rules and to develop recommendable communication and information policy related to fiscal policy.

rors, bottlenecks and cognitive limits within a set of administrative organisations, see on this approach McGuire 2011 in which a theoretical framework and an analyses of policies of environmental sustainability is presented.

⁵⁰ National Audit Office of Finland Performance Report of 2012, for which a systematic selection of performance audit recommendations was taken and the implementation of the recommendations followed up, valtionalouden tarkastusvirasto 2013a. On the actual weakening of the information and evidence-basis of governmental policy-preparation and for a wider discussion on the challenges and problems of knowledge based policy-making in Finland, see the National Audit Office of Finland Annual Parliamentary Report for 2013 Parliamentary Session, Parliamentary Report K 18/2013 vp., see valtionalouden tarkastusvirasto 2013b.

⁵¹ Valtionalouden tarkastusvirasto 2013b.

⁵² Pöysti 2004, p. 562.

3.2. Liberal and deliberative democracy and the role of citizens communicational rights

Citizens' communicational rights and informed citizenship relate to the wider issue of informational fairness and the question concerning models of democracy and representation of power. Democracy has many variants. Each of them has a slightly different representation of power and, places different theories of legitimacy and accountability at their centre.⁵³ The whole concept of legitimacy is open-ended. The legitimacy arrangements in the European economic and monetary union are different in the economic and monetary union and differ considerably from the rest of the institutional structures of the European Union. In the economic union, the legitimacy via the Member States and their governmental action is emphasised.⁵⁴ Despite the nice-sounding call of national sovereignty, the inter-governmentalism may also be a source of legitimacy problems unless it is connected with transparency and public debate enabling accountability.

Legitimacy may be seen to vest either on voluntarism or delegation, participation or efficiency in problem-solving and governance.⁵⁵ In the participation model the exercise of power is approved and performance of the power-wielders is evaluated by those who are affected by the exercise of power whereas in the delegation model exercise of power is approved and evaluated by those who delegate decision-making. Models are very different in transnational relations where the, following cross-border externalities and impacts, those affected may be different than the electoral constituency of the decision-makers.⁵⁶ The liberal democracy based on checks and balances, of which majoritarian rule with parliamentary or presidential decision-making are the main varieties, and the deliberative democracy are different conceptions of democracy. In more philosophic terms, a distinction between modern liberalism and republicanism can be made depending, among other issues, on whether the individual fundamental rights and individual liberties in current market economy or the political autonomy of the political community and the political rights of its citizens have primacy among the constitutional principles of a polity.⁵⁷ Voluntarism ultimately comes back to the legitimacy of the constitution of the political community. Participation may be participation to the decision-making or participation to and enjoyment of the effects of the policies of a polity.

In the context of the European Union, which is a hybrid governance arrangement, all models of legitimacy and democracy have some explanatory and normative force. European Union, however, has a tendency to emphasise out-puts, the good societal effects of the European integration, as the ultimate source of legitimacy.⁵⁸ This would put the communication about the benefits and virtues of the European integration at the centre of the substantive communication policy, that is, establish a project of informing and educating rather than enabling participation. The virtuous character of the overall objectives and results of the European integration even legitimize to a certain extend democratic deficit in terms of participation and classic democratic voluntarism. Legitimacy in a supranational and transnational organisation is itself a challenging issue. The European economic integration in the economic union has put the governments as actors at the forefront. The integration and participation of the citizens may then lag behind.⁵⁹

Liberal theories of power consider power as a competence and ability to influence, to make someone do something what he or she would not do voluntarily. Legitimate power follows from self-

⁵³ Grant & Keohane 2005.

⁵⁴ Tuori 1999. On the recent Finnish constitutional discussion on the democracy and Euro area crises, see Leino-Sandberg & Salminen 2013.

⁵⁵ Boscheck 2006, p. 30.

⁵⁶ Grant & Keohane 2005, 29-34.

⁵⁷ Habermas 2001, p. 766 – 767.

⁵⁸ Boscheck 2006.

⁵⁹ Habermas 2012b.

determination of the individuals who have accepted the exercise of power.⁶⁰ Power is controlled by establishing checks and balances in which the division of state power to separate legislative, executive and judicial arms of government is the fundamental constitutional system of checks and balances. Information and communication has a pivotal role of guaranteeing the functioning of checks and balances. Free and fair elections are at the centre here. Free and fair elections entail the free media and free discussion in the media and the voter's possibility to assess different parties, candidates and their political programmes and also their eventual financial and other connections.⁶¹

Checks and balances and the strengthening of democracy can also improve the fiscal performance measured as fiscal discipline and less volatility on discretionary fiscal policies.⁶² Information about economic policy outcomes and government finances are also considered a key part of the pre-election information. The OECD, for example, recommends as best practise that a pre-election report is delivered to illustrate the general state of government finances before elections.⁶³

In deliberative, communicational models of democracy, power is ultimately the power of free societal argumentation, deliberation, and communicative action which takes place in deliberation.⁶⁴ Legitimacy flows from the public discourse which engages widely society and to which everyone has fair right to participate. Deliberation creates legitimacy. Constitution-writing but also constitution-reading and understanding are performative actions and historical learning processes. Legitimacy is dynamic. Performative action giving legitimacy happens always when a critical reader examines constitutional and institutional arrangements and concludes on their acceptability.⁶⁵ Deliberation is not only a method of constitution-writing but also a method to decide on laws and policies of the polity of the free and equals. Law's role is to establish the rules of the game of practical communicative action and to provide conditions for feeding in material for argumentation in deliberations. This is the particular role of the information and communication policy.

Deliberative theories bridge the participation to the discourse and hence participative rights with the aim of improving the rationality of decision-making. This aspect was also at centre of the thinking of Anders Chydenius, the Diet member who is the father of the publicity principle in Sweden and Finland, concerning the functions of publicity principle. By public reason based on free deliberation, it would be possible to combine the prohibition of the imperative mandate of the elected representatives, and the binding of public decision to the popular will on individual issues. The public debate is the forum which transforms and intermediates public will on individual issues to the elected decision-makers who are subject to prohibition of imperative mandate and only bound by the Constitution and truth as the matter is expressed in Finland's Constitution.⁶⁶ Open competition of arguments in public debate – in deliberation – assures also the rationality of public

⁶⁰ Habermas 2001, p. 766.

⁶¹ Voters' possibilities to assess financial and other connections of political parties, candidates and elected officials are the rationale of the election finance and political financing laws. The right to information enabling this assessment can be seen as part of the right to free and fair elections, see Constitutional Law Committee of the Parliament of Finland, PeVM 2/2009 vp.

⁶² Korkman 2010, p. 48-52. Fatas & Mihov 2003. On the European evidence on the impact of different governance models, see Hallerberg, Strauch & von Hagen 2007.

⁶³ See OECD 2002, chapter 1.6., p. 11. In Finland the National Audit Office of Finland publishes as special parliamentary report an overall assessment of the fiscal policy covering whole electoral period. The report is published two to three months before elections, see *valtionalouden tarkastusvirasto* 2011b.

⁶⁴ Of the several deliberative models of democracy the theoretical version of Jürgen Habermas is well-known, see Habermas 1998.

⁶⁵ See Habermas 2003 and Habermas 2001, p. 775-776.

⁶⁶ On the original and current ideas and functions of publicity principle and a short literature review of the original thinking by Anders Chydenius, see Pöysti 2007.

will and hence public decisions. In deliberative models, the call for participation is stronger than in the voluntarist models of representative democracy. The informational and communicational rights and processes have a central role in the deliberative democracy to provide for and to ensure the conditions for free and rational public discourses.

Deliberation is not a panacea for legitimacy and rationality. The deliberative model can be challenged both theoretically and pragmatically. Deliberations, particularly the practical deliberations in public fora or in the Parliaments, do not always lead to rational or legitimate decisions. Discourses can be manipulated or simply fail. Parliamentary discussions often fail to follow and respect the basic rules of rational practical discourses.⁶⁷

The role of law in the field of information and communication policy is, to the extent possible, constitute the rules of the game and try to rectify the risks of failure and manipulation. This is also visible in the Budgetary Framework Directive 2011/85/EU and Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 which seek to limit the risks of manipulated or over-optimistic economic forecasting and entrust the Independent Fiscal Institutions to produce non-partisan information to the public discussion. The EU's new economic governance rules do not systematically follow the idea of deliberative democracy as a learning process involving citizens. But they do fairly strongly believe in the capacity of deliberation to rationalise economic and fiscal policy-making. While this claim is supported to some extent by the IMF empiric analyses of the impact of the Independent Fiscal Institutions (fiscal councils), the argument is not without problems and considerable challenges.⁶⁸

4. Revised European Economic Governance and conditions for discourses

4.1. Classic issues of fiscal policy as informational and communicational problems

The economic literature and economic policy practises pay increased attention to the issues of political economy and bounded rationality in budgetary processes and other instances of fiscal policy making. A vast economic literature exists to search explanations for biases towards in the longer run undesirable policies. In the fiscal policy area, there is a bias to excessive deficits leading to rising debt-to-GDP ratios and a bias to spend revenue windfalls in good times. According to economic literature, these biases reflect the common pool problem, that is the failure to coordinate competing claims from various constituencies, opportunistic election spending following from politicians' re-election concerns and the imperfect understanding of the government's budget constraint, the fiscal illusion. Over-consumption of public goods leads to expenditure biases.

Over-consumption and over-production may be explained by fiscal illusions. Fiscal illusion follows from the fact that benefits of the public expenditure and services are evident whereas the costs of their production and financing are partly hidden. There is a negative externality flowing from the fact that government spending is often targeted at a specific group in society while it is financed from general tax funds from all tax payers. Consequently, there is an incongruence between those who pay and those who benefit from public spending that translates into the fact that those who benefit from public spending tend to recognise the full benefit of additional spending but only a part of their social costs. Policymakers will then engage in excessive spending since the constituencies they represent do not bear the full social costs of these spending. This externality

⁶⁷ Wiberg 2013.

⁶⁸ The IMF has found that countries with independent fiscal councils, which appear well in the media tend to do better in terms of balance in the size of primary balance, preciseness of economic forecasting and absence of forecasting bias, IMF 2013.

results into excessive deficits and debts.⁶⁹ Weaknesses in the institutional setting and in the architecture of the EU economic and monetary union aggravate biases for deficits, or, do not sufficiently rectify their consequences.⁷⁰ The problem of fiscal illusion is even greater in the tax expenditure, deviations from the normal tax system to promote or favour certain activities, because then the subsidy element avoids normal competition between various needs and may also escape the public criticism on the increase of and level of public expenditures. It is also more difficult to analyse and associate the economic consequences and real costs of the tax expenditure. That is also the economic rationale of Article 14 (2) of the Budgetary Framework Directive 2011/85/EU which requires the publication of the information and overall impact to the government finances of tax expenditure.

In a perfect world of perfect information and fully rational decision-makers budgeting and other occasions of fiscal policy making represent attempt to allocate resources efficiently and increase welfare in the national economy in the most effective way. In this perfect ideal world, voters also associate fully the benefits and costs of public services.

This is not the case in practise. The decision-making on fiscal policy is constrained by lack of information, asymmetric distribution of information, several biases and interest-seeking and electoral captures. Noise blurs signalling and information asymmetries limit the rationality of decision-making albeit the efforts to knowledge-based policy-making. Communication issues are, then, at the central stage.

The recent financial crisis triggered criticism about the economics and in particularly lack of behavioural and psychological perspectives into economic phenomena. However, several problems now at the forefront of the debates of European debt crisis have been identified and discussed in the economic literature a long time ago.⁷¹

Psychological processes leading to economic decision-making are the intermediary through which influence of fiscal policy is partly submitted to economic behaviour. These processes also explain the effectiveness of communication and failures of communication and, hence, provide both positive and normative aspects for the development of communication policies and strategies. Economic psychology aims at understanding the individual behaviour related to economic phenomena.⁷² The financial crisis unfolded in 2008 inspired new research into the psychological and social aspects of crisis and underlying phenomena and into how the public made sense of the crises. This kind of economic psychology is needed in order to understand the emergence of financial and economic crises and how they can be resolved.⁷³

Public sense-making is one of the ways in which the impact of economic and fiscal policies is transmitted to the general public discourse and to political and economic decision-making. Public sense-making, in particular, affects the signalling of fiscal policies. Social representations is a theory of public sense-making enabling a multi-disciplinary perspective to communications and understanding of crises including the psychological processes of making sense. Social representations are shared notions, knowledge, ideas, thoughts and myths about a phenomenon in a social environment. Social representations represent a form of conventional knowledge. They allow individuals to orient within their social environment. The development of social representations include two processes: (1) anchoring in which the individual links knowledge about new phenomena

⁶⁹ Von Hagen & Wolf 2006. Hallerberg, Strauch & von Hagen 2007. von Hagen 2002a. von Hagen 2002b. Velasco 2000.

⁷⁰ IMF 2013, p. 5-7. On the deficit bias see also Calmfors 2005 and Debrun, Hauner & Kumar 2009.

⁷¹ See, for example Calmfors 2005, who takes a pessimistic view to the European Stability and Growth Pact.

⁷² Roland-Lévy, Pappalardo Bourmelki & Guillet 2010 and literature cited there.

⁷³ Gangl et. al. 2012.

to his existing knowledge and (2) objectification in which an abstract phenomenon is translated into concrete and comprehensive entities. Social representations are linked to understanding of society and influence on individual's identity, social group formation and behaviour.⁷⁴ Social representations are, then, a useful concept to the analyses of the communicative action and functioning of democracy in the context of fiscal policy.

Research carried out so far in the context of the financial crisis unfolding in 2008 has revealed differences between lay persons and experts in the representations of the crisis. But there are also interesting similarities across experts and ordinary persons at the street. Both experts and laymen seem to have self-protection biases in which economic shocks are attributed easily to external factors and to persons and actors who do not share the same group as the person himself. In other words, it is easier to blame others than to accept economic measures which affect the daily life and routines of oneself. Both experts and laymen are highly concerned about fairness and, insecure about the possibility to have an economic system in which egoism and immorality of an individual would not endanger the whole economic system. Experts have more confidence on economic recovery than laypersons and laypersons with higher amount of economic knowledge had more confidence. General confidence is necessary for or at least essential aspect of the economic prosperity.⁷⁵ Hence increasing public knowledge about economics would increase general confidence.⁷⁶

Research has also shown that there are noteworthy differences among consumers in relation to credit taking which can be explained by the fear they have for their own position, either to loosing their job or having to use their savings.⁷⁷ People, thus, seem to have a tendency towards risk averseness and that is a factor which will impact empirically felt legitimacy of policy action.

Fear is a powerful motivational factor. Consequently, it is an issue to be taken into account in the analyses of the communicational policies and formulation of normative recommendations on the realisation of democratic principles. This psychological aspect also explains why in practise deliberation and deliberative democracy is neither a guarantee for rational decisions nor a guarantee for an optimal democracy.⁷⁸ Criticisms about deliberative democracy and communicative actions should be taken seriously and knowledge-based decision-making is only a relative normative ideal.

The economic literature on political economy contains an expanding literature on incentives of political actors. Economic models pay increasingly attention to the signalling or communication of policy objectives and outcomes as one of the factors affecting the trade-off between chances of re-election and the most preferred or optimal policies. Voters observe the consequences of the policy actions. Policy-outcomes signal the preferences of the policy-makers. However, voters have generally imperfect information about the politicians' preferences and capability and about policy outcomes. Asymmetries of information affect the trade-off and equilibrium in the rational optimisation of the utility function of the politician and the voter. There is an incentive, depending on the level of risk-averseness of the voters, for policy ambiguity. Voters judge incumbent officials on the basis of policy outcomes, that is, current and lagged economic conditions. Policy tends to respond to assumed public opinion.⁷⁹ Even populism can be, at least partly, explained by informational asymmetries and signalling problems. When voters fear that politicians will be influenced by rich elite, the signals of integrity are valuable. Inequality and weak political and also legal institutions amplify the need to signal integrity. In societies with significant inequalities and lack of

⁷⁴ Gangl et al 2012, 604-605.

⁷⁵ See Akerlof & Schiller 2009. Earle 2009.

⁷⁶ Gangl et al. 2012, 610-613.

⁷⁷ Roland-Lévy et al. 2010.

⁷⁸ See also Wiberg 2013 for another type of approach to the problems of deliberations.

⁷⁹ See Alesina & Cukierman 1990.

voter confidence on the integrity of politicians there are incentives to provide more expansive macro-economic policies than what is the preference of the median voter.⁸⁰

Fiscal illusions and expenditure biases can also follow from the loss-aversion of people. Humans tend to choose the option where big loss is avoided. People evaluate situations with reference points which are shaped by expectations.⁸¹

Institutions and voters' confidence do matter. Institutional factors in particular have a significant impact how different biases in fact influence decision-making on fiscal issues.⁸² Institutional arrangements can change the equilibrium in the utility optimisation performed by voters and politicians.

The incentive for ambiguity explains tendencies to delegate policy and implementation tasks to bureaucratic agencies. Non-elected bureaucrats are preferable for technical tasks in which ability is more important than effort or if there is a significant uncertainty about whether a policy-maker has the required abilities. Politicians are preferable to bureaucrats when flexibility is valuable and time inconsistency is unlikely to be a relevant issue, if vested interests do not have a large stake at policy outcomes. Also the ambiguity and clarity of criteria of fairness impacts the equilibrium concerning delegation to elected officials or bureaucrats in favour of the elected politicians. Imperfect monitoring and thereby imperfect information on the abilities and impacts affects the equilibrium.⁸³

Improved transparency of fiscal policy and budgets is a potential remedy to the fiscal illusion problem and expenditure biases following from it. Increased transparency and more efficient communication may also help to overcome biases resulting from loss-aversion of people by providing better quality reference values and expectation values. The information improving budgetary transparency should not only be objective but appear to be non-partisan and neutral. This creates the case for independent budget offices and Independent Fiscal Institutions providing decision-makers and the general public information about costs and future developments and which due to their expertise and professionalism would have credibility and trust among decision-makers and members of the public.

In economic literature and economic policy practice attention has been therefore paid recently to the establishment and merits of independent fiscal policy institutions to improve transparency and informational bases of decision-making and to rectify some of the rent seeking problems in fiscal policy decision-making. Independent institutions have a variety of tasks but their role is either to monitor compliance with the fiscal rules and to evaluate the effectiveness of fiscal policies or to provide forward-looking policy advice based on economics expertise and research and to provide independent, professional forecasts and analyses of costs and consequences of various policy options.⁸⁴

Improved budgetary transparency is also a way to internalise rent-seeking and serving short term interests in the fiscal policy making. Improved transparency neutralises immediately the benefits of direct manipulation. But transparency and improved public debate can also provide an efficient sanction against rent-seeking and provide even an arena for the perspective of the future generations to be present in the debate. Hidden costs and rent-seeking are made visible and thus a political price is attached to them. There is also evidence that countries with higher level of transparen-

⁸⁰ Acemoglu, Egorov & Sonin 2013.

⁸¹ See Marzilli Ericson & Fuster 2011 where experiments follow the classic theory of Kahneman and Tversky 1979. See also Kahneman & Tversky 1984.

⁸² From the political economy perspective in macro-economic context, see Alessina, Ardagna & Trebbi 2006.

⁸³ Alesina & Tabellini 2007.

⁸⁴ IMF 2013.

cy and good administration have a significantly lower public debt to GDP ratio compared to countries with lesser transparency. Corruption and lower level of good administration and good government significantly influence the economic growth and fiscal balance.⁸⁵

The models of political economy together with behavioural and psychological economics show the practical difficulties in the implementation of the deliberative ideal of democracy. On the other hand, the political economy shows the importance of communication of fair information about the policies to the electorate in order to have the public opinion building and the influence of public opinion to public decision-making to function in accordance with democratic principles. Models in the literature and empiric findings on the decision-making psychology show the value of improving general information about the economic situation, signals on the ability of policy-makers whether they are elected officials or bureaucrats and on the performance of policies for both to the functioning of democracy in accordance with normative democratic principles and also for the macro-economic policy outcomes.

In short, a recommendation that general information about the economic situation and the outcomes of economic policy should be strengthened, that transparency should be increased and the democratic institutions shall also be reinforced, seems to be well-founded also from the perspective of the effectiveness of fiscal policy in terms of long term financial sustainability. Information policy and citizens' informational rights are at the centre of reconciling democratic ideals and the quest for sustainable fiscal policy.

4.2. The potential of deliberative democracy in the revised European economic governance

The European Union Stability and Growth Pact is a rule based framework for the setting and assessing of fiscal policies in the European Union.⁸⁶ The Stability and Growth Pact consists of legal rules expressed in the Union legislation and of political additional commitments, in the Resolution of the European Council convened at Amsterdam (1997) and in the report presented by the ECO/FIN Council and acknowledged by the European Council in 2005. A Code of Conduct on technical specifications on the implementation of the Stability and Growth Pact complements the rule framework. The core of the Stability and Growth Pact is constituted by two Council Regulations, which, in the course of the development of the Stability and Growth Pact, have been amended in 2005 and, after the financial crisis have been complemented by new provisions in 2011 (the so called Six Pack) and 2013 (the so called Two Pack). The core of the Stability and Growth Pact are:

- Council Regulation (EC) No 1466/1997 EC of 7 July 1997 on the strengthening of the surveillance of budgetary positions and the surveillance and coordination of economic policies. This regulation is the core of the preventive arm of the Stability and Growth Pact. Regulation has been amended in 2005 and 2011 reforms of the Stability and Growth Pact. The overall aim of the Regulation and of the preventive arm of the Stability and Growth Pact is to coordinate fiscal policies of the Member States and to ensure that budgetary policy leads to sound medium term budgetary policy.
- Council Regulation (EC) No 1467/97 of 7 July 1997 on speeding up and clarifying the implementation of the excessive deficit procedure. This regulation is the core of the corrective arm of the Stability and Growth Pact and deals with the situations in which a

⁸⁵ See, for example, analyses by Korkman 2010, p. 52 on transparency and debt to GDP, and Hillman 2004, Kauffman & Vicente 2011, Méndez & Sepúlveda 2006, and Mauro 1995 on the impacts of good vs. bad administration, in particular corruption.

⁸⁶ European Commission 2013a, p. 5.

Member State exceeds the reference values set by the Treaty. Regulation sets the procedures to be followed in such situations. The aim is to correct gross policy errors. The regulation has been amended in 2005 and 2011 reforms.⁸⁷

The history of the Stability and Growth Pact has been one of international and institutional learning process. The history of the Stability and Growth Pact shows also the limits of knowledge based policy making in two terms: the knowledge-based policy making does not refer to the use of perfect or what retrospectively appears to be even good knowledge but to the effort of using of the best possible knowledge at the time. Limits of the knowledge-based policies also result from the fact that political consideration of societal justice and fair distribution override technocratic knowledge. In the context of the European Union, the consideration for the sovereignty of the Member States and balance of power calculations also limit additionally the realm of the rational reason of economic knowledge.

In 2005, the Stability and Growth Pact was reformed with the intention to enhance the economic rationale and provide greater flexibility. Background to reform was also the compliance problems of which the most notable examples are the excessive deficit procedures of France and Germany in 2003, which also led to the European Court of Justice judgement. The European Court of Justice in its judgment among other things underlined the legal and binding nature of the Treaty provision on economic policy coordination and excessive deficit procedure and of the legal nature of the Council Regulations in the Stability and Growth Pact.⁸⁸

The uniform rules in the preventive arm of the Stability and Growth Pact were replaced with differentiated rules aiming to take into account a country-specific situation. The requirement of achieving the Treaty reference value of maximum public deficit of 3 % within a fixed timeframe was replaced with the requirement of a fiscal effort as measured by the structural deficit. Each Member State should establish a Medium-Term Budgetary Objective (MTO) set country-specifically in structural terms. Structural balance is a theoretical concept which cannot be directly measured or accounted. It is a result of fairly technical calculation based on several assumptions. Shortly and popularly defined, it means general government balance corrected with the impacts of the cyclical element following from the economic cycle and from the impacts of once-off items.⁸⁹ The setting of the close to balance budgetary rule in structural terms was the innovation in 2005 and not a novelty brought by the 2012 conclusion of the Fiscal Compact. Theoretically, this allows cyclical or Keynesian economic policy but creates considerable problems of understanding and communication outside the economists' expert community. Calculation of structural balance in practise requires several discretionary conventions.

The reforms in 2011 and 2013 brought a broader reform of economic policy coordination and governance albeit reforms were incremental by their nature, seeking to improve the defects of the system rather than to replace the old system with a comprehensively reformed rule framework. A coordinated calendar of European guidance on fiscal economic policy, the European semester of economic policy, was taken into use.⁹⁰ Sanctions were also strengthened and the reversed qualified majority voting, which requires an active qualified majority to turn down Commission proposal, was taken into use.

⁸⁷ European Commission 2013a, p. 7 -9.

⁸⁸ European Court of Justice, Judgment in Case C-27/04, *Commission of the European Communities v Council of the European Union*, ECR [2004] I-06649.

⁸⁹ On the concept and calculation of the structural balance, see National Audit Office of Finland Fiscal Policy Audit on the Computation of the Structural Balance, audit report 13/2013, *valtiontalouden tarkastusvirasto* 2013c. See also European Commission 2013b, 22.

⁹⁰ See European Commission 2013a, graph 1.1., p. 12 for a good graphic presentation of the European Semester.

The reforms of the Stability and Growth Pact have been mainly reactions to the emerging problems and crisis. In 2011, the reform was a reaction to the vulnerabilities revealed in the European debt and financial crisis. The overall goal was to create a greater national ownership and an enhanced enforcement and to provide for smarter fiscal policy rules. Reforms went beyond the Stability and Growth Pact itself with the new Macro-economic Imbalances Procedure and the stipulation of the minimum requirements for national budgetary frameworks in order to secure better adherence to the European fiscal policy rules. The latter is the core objective of the Budgetary Frameworks Directive 2011/85/EU.

The reform in 2013 was a continued reaction to the financial and debt crisis and the objective was to enshrine European Union rules at the national level.⁹¹ First of the Two Pack Regulations, the Draft Budgetary Plans Monitoring Regulation or Enhanced Monitoring Regulation (EU) No 473/2013 imposes the obligation to the euro area Member States to submit their draft budgetary plan to the European Commission for assessment before the adoption of the Member State budget. The Commission may request a new plan if the Commission observes a particularly serious non-compliance with the European policy obligations in the original plan. The Commission publishes its opinion on draft budgetary plans and the purpose is to integrate the Commission opinions to the national budgetary processes.⁹² The Regulation sets also a common timeframe for budgetary plans. The Regulation furthermore requires Member States to establish independent bodies (Independent Fiscal Institutions) to monitor compliance with the Medium Term Objective in accordance with the Stability and Growth Pact and compliance with national numerical fiscal rules as referred to in Article 5 of Budgetary Framework Directive 2011/85/EU. Additionally, the independent fiscal institutions shall monitor the adjustment path towards and correction of deviations from Medium-Term Objective. The independent fiscal institutions shall, thus, monitor both European and national fiscal rules.⁹³ The second of the Two Pack Regulations, Regulation on the Enhanced Surveillance of Member States in Severe Financial Difficulties (EU) No 472/2013 establishes a possibility for the Commission to put a country to enhanced surveillance with the obligation of the Member States concerned to address the sources of financial and economic instability, macro-economic adjustment programmes and post-programme surveillance for Euro Area Member States experiencing severe difficulties with financial stability or in receipt of financial assistance.⁹⁴ The inter-governmental Treaty on the Stability, Coordination and Governance in the economic and monetary union (TSCG) which contains the Fiscal Compact, complements the Stability and Growth Pact by committing the signatories to mirror the key elements of the preventive arm of the Stability and Growth Pact in national law. The Fiscal Compact obliges the signatory Member States to incorporate Medium-Term Objective and adjustment path and the reference values in structural terms into binding national law and to establish an automatic correction mechanism. The common principles of the correction mechanism are set in accordance with TSCG in a Commission Communication.⁹⁵ The correction mechanism required includes the establishment of an independent national monitoring body, independent fiscal institution, and defines requirements for independent fiscal institutions. The Two Pack Regulation replicates this part of the TSCG in Union law.

Stability and Growth Pact and, the additional European Union economic governance rules form a complex entirety consisting of Union legislative acts and inter-governmental treaties beyond the Union law. The entirety is difficult to understand and this crisis legislation does not correspond to

⁹¹ European Commission 2013a, p. 12 – 20.

⁹² Preamble, paragraph 20 and Articles 6 and 7 of Regulation (EU) 473/2013.

⁹³ Article 5 of Regulation (EU) No 473/2013.

⁹⁴ Regulation (EU) No 472/2013 of the European Parliament and of the Council of 21 May 2013 on the strengthening of economic and budgetary surveillance of Member States in the euro area experiencing or threatened with serious difficulties with respect to their financial stability, OJ L 140, 1, 27.5.2013.

⁹⁵ See COM (2012) 342 final.

the European Union's own ideals of clarity and better regulation. The complexity of the economic governance rules may become a problem for their legitimacy – they easily fail in the dynamic learning process in which the citizen could understand and approve the rationale of their contents and existence because of their mere complexity.⁹⁶

The communication policy in the original Stability and Growth Pact was peer review and pressure among transnational networks of government officials, particularly among the finance ministers meeting at the ECO/FIN Council and at the Euro-group. Information policy aimed to create conditions for this multilateral peer review in an inter-governmental network which is a sui generis policy area in the definition of the competencies of the European Union. The Commission and Council recommendations are public documents. The original Stability and Growth Pact did foresee institutional dialogue with the Member States but the national ownership of the Stability and Growth Pact commitments and coordination discourse have remained weak.⁹⁷

The Six Pack and Two Pack reforms of the economic governance added new dimensions to the information and communication policy. Objectives are to strengthen the national ownership of the European fiscal rules and to better integrate European rules and guidance in the national budgetary processes and discourses. Increased transparency and production and dissemination of information to the public, parliamentary and expert discourses are here among the tools used for that purpose. The budgetary Framework Directive 2011/85/EU tries in particular to address the problem of over-optimistic macro-economic forecasts and the founding of fiscal policies to over-optimistic economic scenarios and to improve the quality of forecasting and information bases for European surveillance of fiscal policy and for national fiscal policy-making. Undeniably, the quality of macro-economic forecasts and optimistic biases in them has been a problem in many European countries.⁹⁸ This problem concerns also Finland. The government's fiscal policy has during the electoral period 2007-2010 and 2011 – 2014 been based on higher expectations on economic growth than what has been realised.⁹⁹ In the case of Finland, the primary problem is not in the quality of macro-economic forecasting but governmental programmes (coalition agreements) that have defined the basis for economic and fiscal policy to be higher than expected economic growth. In addition, the realised economic growth has been below original forecasts.¹⁰⁰ In the Six Pack and Two Pack legislation, the availability of data is seen as a crucial factor for a proper European budgetary surveillance framework. Transparency is also seen as a key to the quality of statistical data.¹⁰¹

The Six Pack and Two Pack follow the logic that there shall be public discussion on European policy rules and policy goals both at the Union institutions and at the Member States and information and the communication policy stipulated in the Union legislative act follows this general idea. This is a good approach given the challenges of democratic legitimacy in the context of glob-

⁹⁶ Compare Habermas 2001 and 2003 on the dynamic nature of legitimacy in communicative action; the performative act creating legitimacy takes place also when reading and approving the principles underlying a constitutional text, not only when the constitutional text is originally written.

⁹⁷ European Commission 2013a.

⁹⁸ Frankel & Schreger 2013.

⁹⁹ See the macro-economic forecast of the Bank of Finland, Suomen Pankki 2013, p. 33. According to the Bank of Finland the Government based its policies in electoral period 2007-2010 to assumption of the growth of the value of the GDP to be 10 % whereas the realised growth was approximately 1 ½ %. The Government Decision on Fiscal Ceilings for years 2013 – 2016 anticipated the GDP growth in the period to be 21 % whereas according to the Christmas 2013 economic forecast of the Bank of Finland the GDP growth is expected to be 13 %.

¹⁰⁰ See National Audit Office of Finland Fiscal Policy Audit Electoral Period Report to Parliament in 2011, Parliamentary Reports to 2010 parliamentary session, valtiontalouden tarkastusvirasto 2011b. See National Audit Office of Finland, Fiscal Policy Audit Mid-term Report of the 2011 – 2014 Electoral Period, Parliamentary Reports to 2012 parliamentary session, valtiontalouden tarkastusvirasto 2013d, p. 17-19.

¹⁰¹ COM (2010) 523 final. Preamble of Directive 2011/85/EU, paragraphs 4, 8- 12.

alisation of economy and change of the European Union. The underlying challenge is the asymmetry between the social, societal and economic forces which operate at the transnational space between nation states and the capacity for transnational governmental action on the one hand and, on the other hand, the legitimate transnational political action by the citizens.¹⁰² European integration and politics have had and still have a technocratic character. Consequently there is also a considerable risk in the new economic governance arrangements of strengthening the executive powers to the detriment of democratic legitimacy and powers of the national parliaments.¹⁰³ To overcome the asymmetry and democratic deficit, the citizens' should be brought into the transnational politics. Since the Member States are the central polities in the European Union, this means that the European political topics shall be brought into the national arenas and medias of political debate.¹⁰⁴ The Budgetary Framework Directive 2011/85/EU and the Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 aim exactly to contribute to that. However, they see transparency and public debate as teleological tools to improve long-term sustainability of the public finances and functioning of the coordination of budgetary policies of the Member States and adherence to the European fiscal rules rather than as genuine democratic ideals on their own right.

The Budgetary Framework Directive 2011/85/EU establishes categories of data and background data and comparative information which shall be made public and easily available for public and expert discourses. Member States shall have comprehensive and consistent public accounting systems subject to internal control and independent audits and ensure timely and regular availability of fiscal data for all sub-sectors of general government. Member States shall also publish cash-based fiscal data monthly for central government, state government and social security subsectors and quarterly for the local government. As background information the cash-based data and data based on ESA 95 standard on statistical national accounts shall be reconciled.¹⁰⁵ The Directive sets qualitative principles concerning realistic macro-economic planning and macro-economic and budgetary forecasting. Forecasts shall be realistic and use most up-to date information. Budgetary planning shall be based on the most likely macro-fiscal scenario or on a more prudent scenario. Member States shall compare the macro-economic and budgetary forecasts to the most updated Commission forecasts and the forecasts produced by independent bodies if they produce their own forecasts, and the significant differences between the chosen macro-fiscal scenario and the Commission forecast shall be described with reasoning.¹⁰⁶ The official macro-economic and budgetary forecasts used for fiscal planning shall be made public (the forecast itself) and also Member States shall make public methodologies, assumptions and relevant parameters underpinning the forecasts. The Commission shall also make public the methodologies, assumptions and relevant parameters underpinning its forecasts.¹⁰⁷ In practise, the Commission also makes available applications used in the Commission forecasts as part of the transparency of the methodologies. Access-to-information means thus auditability, assessability and controllability of the quality of information and access to back-ground methodologies including applications used to produce the Macro-economic forecasting shall be subject to regular evaluation. The results of the evaluation shall be made public.¹⁰⁸ Forecasting shall also contain analyses of alternative scenarios taking into account

¹⁰² Habermas 2012a.

¹⁰³ Habermas 2012b.

¹⁰⁴ Habermas 2012b, p. 488 in which Habermas writes about the democratic deficit and the management of European debt crisis: "What have been missing until now are national public spheres in which discussion and will-formation on European topics can be conducted. Different media are not required for this, only a different practice on the part of the existing media."

¹⁰⁵ Article 3 of the Directive 2011/85/EU.

¹⁰⁶ Article 4 (1) of the Directive 2011/85/EU.

¹⁰⁷ Article 4 (2) and 4 (5) of the Directive 2011/85/EU.

¹⁰⁸ Article 4 (6) of the Directive 2011/85/EU.

risk scenarios and sensitivity analyses.¹⁰⁹ The Budgetary Framework Directive hereby establishes categories of data and contextualised background data what the Member States shall make publicly available. Directive thus, concerns directly the openness and transparency of the Member State budgetary processes.

The Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 sets additional publication requirements for the Member States. Member States shall produce draft budgetary plans in a common European timetable (before 15 October) covering the whole general government and its sub-sectors and subject them to assessment by the European Commission. The Member States shall also publish these draft budgetary plans, which shall not be confused with the Budget Bills submitted to the Parliaments and other decision-makers. Draft budgetary plans referred to as Regulation are summary synthesis of core economic and fiscal policy objectives and forecasted fiscal and economic outcomes and budget outturns (budgetary balance of each sub-sector of the general government) and summary of the main budget data on the aggregated macro-economic level. The Regulation contains a detailed list of economic and budgetary data which shall be part of the draft budgetary plan.¹¹⁰ In addition to core data, the Regulation requires inclusion and publication of key underpinning background data as part of the draft budgetary plans. This contextualising background data concerns (1) the main assumptions of the independent macroeconomic forecasts and important economic developments which are relevant to the achievement of the budgetary targets; and (2) the methodology, economic models and assumptions, and any other relevant parameters underpinning the budgetary forecasts and the estimated impact of aggregated budgetary measures on economic growth.¹¹¹

The Regulation requires the Member States to base their national medium-term fiscal plans and draft budgetary plan to an independent forecast or forecast endorsed by the independent body.¹¹² The Regulation contains a definition of and requirements of the independent bodies, independent fiscal institutions.¹¹³ The Commission's assessment of the Member States draft budgetary plans is also published and specific dialogue procedures between the Commission and the Member State Parliament seek to bring in the European guidance on fiscal and economic policy as part of the national public and parliamentary debate.

The core of the Budgetary Framework Directive 2011/85/EU is the requirement of the Member States to establish national numeric fiscal policy rules covering the whole general government (public sector) and its sub-sectors. While this is not an information policy rule as such, it strengthens its overall openness by obliging open target-setting in the fiscal policy. Monitoring of compliance with fiscal rules shall be carried out by independent fiscal institutions. Also Member States shall have a multiannual fiscal planning system which is called medium-term budgetary frameworks. Chapter VI of the Directive sets additional transparency and information policy requirements for the Member States concerning extra-budgetary bodies and funds, contingent liabilities and tax expenditure. The coordination mechanisms shall ensure a comprehensive and consistent coverage of the multiannual budgetary framework and fiscal planning and forecasting. General government bodies and funds which do not form part of the regular budgets and the combined impact of those bodies and funds to government balances and debts shall be disclosed. Detailed information of tax expenditure (tax subsidies) on revenues shall be published as well as information

¹⁰⁹ Article 4 (4) of the Directive 2011/85/EU.

¹¹⁰ Article 6 of the Regulation (EU) No 473/2013.

¹¹¹ Article 6 (3) paragraphs f and g of the Regulation (EU) No 473/2013.

¹¹² Article 4 (4) of the Regulation (EU) No 473/2013.

¹¹³ Article 2 and Article 5 of the Regulation (EU) No 473/2013.

on contingent liabilities including government guarantees, non-performing loans and liabilities stemming from the operation of public corporations.¹¹⁴

Eventually, a very significant information policy deriving from the Directive is the adoption and taken into use of common European Public Sector Accounting Standards (EPSAS-standards) in all public sector bodies in the European Union Member States. The Directive required the Commission to assess the suitability of International Public Sector Accounting Standards (IPSAS) for Member States.¹¹⁵ The Commission's assessment sees the need for adoption of EPSAS on the basis of IPSAS in order to improve the quality of government finance statistics and comparability of the financial information across the borders.¹¹⁶

The Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 requires the establishment of independent national bodies, Independent Fiscal Institutions, to monitor both the attainment and adjustment path towards the medium-term objective (MTO) defined in accordance with the Stability and Growth Pact rules and the compliance with the national fiscal rules set in accordance with the Budgetary Framework Directive. Independent Fiscal Institutions shall also monitor the activation and functioning of the correction mechanisms in cases of significant deviation from the medium-term objective or adjustment path towards it.¹¹⁷ The macro-economic forecasts shall be either produced or endorsed by an independent body, which does not necessarily need to be the same as the independent fiscal institution set for the monitoring. Independent Fiscal Institutions – according to the terminology of the Regulation independent bodies – are bodies which are structurally independent or endowed with functional authority vis-à-vis the budgetary authorities. The independence shall be guaranteed by law or statutory regime with binding administrative provisions. They shall be independent in their discharge of duties, have adequate resources and appropriate access to information to carry out their mandate. Members shall be appointed on the basis of experience and competence. The Independent Fiscal Institutions shall, in particular, have the capacity to communicate publicly in a timely manner.¹¹⁸ This part of the Regulation incorporates into Union law the provisions of the Fiscal Compact in the TSCG Treaty. The Fiscal Compact requires balanced budget rules, set as the maximum structural deficit, in accordance with the minimum requirements of the Medium-Term Objective with automatic correction mechanism to be defined by national law, preferably of constitutional character. The correction mechanism shall be defined in accordance with the common principles set pursuant to TSCG Treaty. The common principles on the correction mechanism are defined in the Commission communication.¹¹⁹ Principle 7 on the Independent Fiscal Institutions monitoring is essentially incorporated to the text of Regulation (EU) No 473/2013.

Academic literature has considered whether fiscal policy could be delegated to an independent authority like monetary policy is delegated in the economic and monetary union to an independent central bank.¹²⁰ The establishment of prior decision-rules, which also communicate the policy-objectives and policy action and thereby influence the expectations and behaviour of the economic

¹¹⁴ Articles 13 and 14 of the Directive 2011/85/EU.

¹¹⁵ Article 16 (3) of the Directive 2011/85/EU.

¹¹⁶ COM (2013) 114 final. The issue was subject for a high level conference in May 2013 in which among others President of the European Council, Herman van Rompuy, expressed his support for the common European Public Sector Accounting Standard from the angle of the needs of decision-makers in economic policy, see the proceedings of the conference at <http://epp.eurostat.ec.europa.eu/portal/page/portal/conferences/introduction/2013/epsas#7> (page visited 28.12.2013). On the arguments for and needs of EPSAS, see also Pöysti 2013, p. 75-77.

¹¹⁷ Article 5 of Regulation (EU) No 473/2013.

¹¹⁸ Article 5 of Regulation (EU) No 473/2013.

¹¹⁹ COM (2012) 342 final.

¹²⁰ IMF 2013, p. 6 quotes some literature on this; see more comprehensively Debrun, Hauner and Kumar 2009.

actors, has however, been the general approach of trying to solve the expenditure biases.¹²¹ Delegation of some aspects of fiscal policy to an independent authority can be dismissed both on positive and normative grounds since such delegation is likely to lack credibility and since fiscal policy is to a large extent distributive, which means, that without violation of the democratic principles and democratic legitimacy, delegation to an unelected authority is not acceptable and politicians prefer not to delegate distributive tasks. A bureaucratic decision-making is preferred when technical ability is a key issue. A bureaucratic decision-making on redistribute tasks would be acceptable if what is “fair” redistribution could be clearly specified *ex ante* and the bureaucrat could be trusted to implement them.¹²² In literature, however, there are also proposals that only the setting of the appropriate size of the budget and budget balance would be delegated whereas the distribution would still be subject to democratic decision-making.¹²³ Albeit in no country there is delegation of any aspect of the fiscal policy to an unelected expert agency, academic discussion on the merits and deficits of such agency is relevant for the analyses of the European economic and monetary union. The strengthened monitoring powers of the European Commission and the Council empower the executive over Parliaments and represent some elements of delegation of fiscal policy to an unelected executive authority.¹²⁴

In economic literature and in several international policy documents, of which drafters of the Regulation (EU) No 473/2013 have been informed, the production and the dissemination of information as well as the setting of fiscal policy rules and the establishment of softer independent watchdogs are seen as a way to overcome expenditure biases in economic policy. In practise, including in the TSCG, the Budgetary Framework Directive 2011/85/EU and Draft Budgetary Plans Monitoring Regulation (EU) No 473/2013 and in the establishment of fiscal councils or Independent Fiscal Institutions, an approach of persuasion and influence through public debate and expert discourses has been adopted.

Fiscal councils or independent fiscal institutions are independent public institutions aiming at promoting sustainable public finances through various functions, including public assessments of fiscal plans and performance, and the evaluation or provision of macroeconomic and budgetary forecasts.¹²⁵ By fostering transparency and promoting a culture of stability, they can raise reputational and electoral costs of undesirable policies and broken commitments. Independent fiscal institutions do not have delegated decision-making. Thereby they fundamentally differ from the academic ideas of delegated decision-making. The independent fiscal institutions or fiscal councils have a variety of different institutional arrangements but a common feature is the independence or at least the functional independence from the government. The functions of independent fiscal institutions are to improve policymakers’ incentives to opt for sound fiscal policies. This is done by fostering transparency over the political cycle and by improving democratic accountability.

¹²¹ IMF 2013, p. 6-7.

¹²² Alesina & Tabellini 2007.

¹²³ Korkman 2010, p. 59 – 60 on the review of ideas in presented in literature.

¹²⁴ Jürgen Habermas rightly warns about the excessive strengthening of the executive in the management of European debt and fiscal crisis, see Habermas 2012a.

¹²⁵ The OECD calls the independent fiscal policy watchdogs, fiscal councils, as Independent Fiscal Institutions, see OECD Principles for Independent Fiscal Institutions, OECD 2013. The IMF definition of fiscal councils reads as follows: “A fiscal council is a permanent agency with a statutory or executive mandate to assess publicly and independently from partisan influence government’s fiscal policies, plans and performance against macroeconomic objectives related to the long-term sustainability of public finances, short-medium term macroeconomic stability, and other official objectives. In addition, a fiscal council can perform one or several of the following functions: (i) contribute to the use of unbiased macroeconomic and budgetary forecasts in budget preparation (through preparing forecasts, or proposing prudent levels for key parameters), (ii) identify sensible fiscal policy options, and possibly, formulate recommendations, (iii) facilitate the implementation of fiscal policy rules, and (iv) cost new policy initiatives”, IMF 2013, p. 8.

Critical public assessments based on objective criteria discourage opportunistic shifts in fiscal policy, for example a pre-electoral spending spree. Independent fiscal institutions increase through their independent analysis, assessments, and forecasts public awareness about the consequences of certain policy paths, contributing to a stability culture that directly addresses fiscal illusion. Hence the reputational and electoral costs of unsound policies and broken commitments can be increased and incentives for sound fiscal policies improved. All these functions and effects realise through public discourses and can be also related to the deliberative models of decision-making. The independent fiscal institutions can also provide direct inputs to the budget process and participate to the expert and managerial discourses of policy-drafting by, for example, producing or endorsing independent macro-economic forecasts and/or to assess structural balance. In doing so, the independent fiscal institutions relate directly to the institutions and models of knowledge-based or evidence-based decision-making.¹²⁶

Independent fiscal institutions make their contribution through improvement of the quality of information in the decision-making process (technocratic dimension) and through enlightening the public debate (deliberative dimension). They are a specific type of institution and very close to the Supreme Audit Institutions responsible for the external government audit. Independent fiscal institutions are an important element of the information and communication policy based on law.

The empiric evaluation of the effectiveness of the existing independent fiscal institutions shows that their success also depends on the communication. According to a study conducted at the IMF, those Independent Fiscal Institutions which have a strong presence in the public debate with an effective communication strategy seem to make the best contribution measured in terms of the level of the primary balance of the general government and the quality of macro-economic and budgetary forecasts measured as absence of biases and precision of forecasts - the presence in the public debate was measured in terms of quotes in the media. In addition, there are several principles of design and functioning which contribute to the effectiveness: Clear official mandate to evaluate adherence to the fiscal policy rules and contribute to the public debate, technical capacity and, in particular strong independence and non-partisan approach.¹²⁷

But the independent fiscal institutions do not deliver the expected result alone. Good statistical governance systems and a solid public financial management system ensure clear policy targets and the availability of good data all which are prerequisites for good fiscal performance measured as the size and balance of the general government primary balance and absence of biases and forecasting errors in budgeting.¹²⁸ The sustainability of fiscal policy and also the conditions for success of independent fiscal institutions seems, thus, be connected to the overall realisation of good administration and functioning of constitutional democracy.¹²⁹ The finding is consistent with earlier empiric economic literature which shows that institutional rules and factors which limit excessive discretion provide for better long-term economic welfare measured in terms of economic growth.¹³⁰ This is also an important lesson for the European Union in the implementation of the Independent Fiscal Institutions and the revised economic governance rules in general.

¹²⁶ IMF 2013. Recent empiric evidence shows that the presence of Independent Fiscal Institution in a country reduces over-optimistic biases in macro-economic forecasting, see Frankel & Schreger 2013 in which also the forecasting biases in Eurozone was analysed.

¹²⁷ IMF 2013, p. 26 – 34.

¹²⁸ IMF 2013, p. 41.

¹²⁹ On the relevance of good administration to fiscal policy in the European Union, see Pöysti 2013.

¹³⁰ See, for example, a study by Fatas & Mihov 2003.

5. Good communication policy regarding uncertain future

The communicational challenge in the quest for sustainable fiscal policy and knowledge-based fiscal policy making is how to present complex realities with uncertainties and how to make them understandable to political decision-makers and to the citizens. Success in this communication is also a *conditio sine qua non* for the substantive legitimacy of the long- and medium-term fiscal decision-making.

In the revised European Union economic governance, the role of the fiscal policy rules is strengthened and the fiscal policy rules are constitutionalised, representing an additional dimension of substantive constitutionalism. The function of the fiscal policy rules is to limit policy-making discretion and internalise to the decision-making the long term perspective. Role of the fiscal policy rules is to increase the credibility of fiscal policy but also an expression of commitment and communication. Through the rules the decision-makers commit themselves to and signal clear policy objectives. Good fiscal policy rules are able to solve the biases-problem they are set to solve, they are clear and transparent.¹³¹ The success of the fiscal policy rules in overcoming fiscal illusions and limiting expenditure biases in decision-making depends on the transparency and anchoring of the policy rules in the expectations of policy-makers, voters and economic actors.

The success of the fiscal policy rules and, as shown in previous chapter, the success of Independent Fiscal Institutions depend on the communication strategies and on the realisation of the citizens' communicational and informational rights. However, this is not straightforward, since in the good communication strategy of liberal constitutional governance, the optimal conditions for the realisation of the citizens' political autonomy and self-determination and the citizens' communicational rights should be given but, at the same time, the restrictions in cognitive capacities of the different target audiences and information processes should also be taken into account. The non-partisan nature requires fairness and avoidance of manipulation, or a bias in the communication. The complexity of the reality and uncertainties of the future should be communicated fairly but in understandable terms.

The ideals of knowledge-based decision-making and communication policy may sometimes knowingly or unknowingly depart from the assumption of a knowable world – that is a world in which one can make sense- a world in which societal topics can be known and communicated about clearly- a world in which a common interpretation can be made in communication and dialogue. Our contemporary, inter-connected and digital network society with over-flood of information and wicked problems is not such a world. The problem of communicators and communication policy makers is rather the world of wicked problems with many uncertainties and in which many issues are difficult to know.¹³² In times of great uncertainties and paradigmatic changes, what counts as good communication policy is necessarily different. Good communication policy reflects paradigmatic structures of society, economy politics and law, technology being one of the main paradigmatic drivers for change.

An example of the challenges in communication and creating governmental action on the basis of the information reported is the question of the sustainability of public finances. A short popular definition of sustainability is that public finances are sustainable when public debt is manageable in the longer run. But what is manageable is a matter of convention. And the calculation of the future cash flows depends on several assumptions. The sustainability calculations are then very sensitive to changes in parameters and assumptions. In the Finnish debate, the sustainability gap is

¹³¹ National Audit Office of Finland: Fiscal Policy Audit Electoral Period Report 2007-2010, *valtionalouden tarkastusvirasto* 2011b, p. 41 and 57.

¹³² See *valtionalouden tarkastusvirasto* 2013b, p. 11-25.

described in the Ministry of Finance official documents as the surplus in terms of the percentage of the GDP which would guarantee that public finances would be stabilised without increasing the tax rate or level of public debt or weakening the public services. A single figure on the sustainability gap is given. The Finnish Ministry of Finance definition comes close to the indicator S2 used by the European Commission in the European assessments of the long-term sustainability of public finances.¹³³ The concept sustainability of public finances itself is a multi-dimensional one. The European Commission has distinguished different temporal and substantial dimensions in the issue of the sustainability of public finances. The short term sustainability is measured by the indicator S0 which is a composite indicator describing financial stress of the government. The medium-term sustainability is measured with the indicator S1, which shows the budgetary adjustment effort required in terms of steady improvement in the structural primary balance of the general government to be introduced until 2020 and then sustained over a decade, to bring debt ratios back to 60 % of the reference value stipulated by the Treaty on the Functioning of the European Union. In other words, the S1 measures the required fiscal adjustment in structural terms to reach the Treaty reference value by 2030. The long-term sustainability indicator S2 used by the European Commission shows the adjustment to current structural primary balance to fulfil the infinite horizon intertemporal general government budget constraint. The intertemporal budget constraint is satisfied when the projected outflows of the government (current public debt and the discounted value of all future expenditure, including the projected increase in age-related expenditure) are covered by the discounted value of all future government revenue. It considers the projected expenditure to 2060 and beyond.¹³⁴ All indicators are presented as single figures.

The practise of presentation of exact figures on the sustainability gap without consideration of alternative scenarios and policies figures has been criticised in academia.¹³⁵ The single figures can be considered as over-simplistic truths. The presentation of sustainability calculations as single figures ignore that in the course of the time decisions will necessarily be made which change the picture. Single figures do not disclose a reliable view of the phenomena. Sustainability calculations are not single scenarios and not forecasts. Similar problems of presentation are also related to economic forecasts. In them also a forecasted figure is presented but the forecasts are only able to capture a certain range of confidence of values with certain probabilities. Concerning sustainability calculations, the government's fiscal limits for taking new debt is not a single point: it is a probability distribution, a feature that carries important implications for thinking about fiscal sustainability.¹³⁶ One possible way to look into sustainability is to perform a stochastic analysis with probabilities on how far the government debt could go and when risk neutral investors will cease lending and define a fiscal space on the basis of that.¹³⁷

Governments will also with some probabilities react to the debt and carry out fiscal adjustments. There are also possibilities to perform sustainability analyses which take the probabilities of adjustment and policy behaviour into account.¹³⁸ Information seeking to give a realistic and thus fair view is full with uncertainties, and these uncertainties should also be communicated beyond the academic community of experts.

¹³³ On the Finnish Ministry of Finance calculation approach, see valtiovaraministeriö 2013b, p. 92-97.

¹³⁴ European Commission 2012, p. 5-7 and more comprehensively p. 17 – 24.

¹³⁵ In Finland, professor Pertti Haaparanta has been very critical towards the sustainability analysis presented by the Finnish Ministry of Finance, criticising them of not being made in accordance with the recommendations presented in economic study books and lack of background information and analyses of alternative scenarios, see Haaparanta 2011.

¹³⁶ Leeper 2013.

¹³⁷ Ghosh et. al 2013.

¹³⁸ See Bi, Leeper & Leith 2013. Bi & Leeper 2013.

When the exact figures are at best medians or averages of probabilities or describe in numeric terms what would be the consequences of the current policies if they are continued as they stand today, it is fairly easy to challenge them from a chosen angle and assumptions. Then their reliability as indicators and conveyers of an important message can be called into question. In that case the figures do not any longer help in the creation of common understanding the future challenges. A practical example was seen in 2011 in Finland in the negotiations for the governmental programme. The drafters of the coalition agreement could not agree on the size of the sustainability gap.¹³⁹ The human mind has limited cognitive capabilities and, hence, there is a semi-natural tendency to look after understandable single figures. That is also why there is a demand for a single, capturing figure.

Indicators and estimates on the sustainability of public finances are sensitive to the general government's financial position at the year which is the starting point of the sustainability assessment. In addition, they are very sensitive to assumptions made in the calculation exercise. Firstly, assumption sensitive points in the estimation of the sustainability of public finances is, among other issues, the estimation of the potential growth of GDP. The second source of particular uncertainty is the evolution of aging related costs, i.e. is health care and social care in the future years. Thirdly, the population scenario itself is only a projection and time series in Finland tell that there are significant errors in population forecasting. Single estimates on the sustainability indicators hide the uncertainty and also structural issues which underlie the issue of sustainability. The significance of the financial position of the general government in starting year of the projection also means, that under the conditions of good economic growth and good financial position of the general government may hide structural weaknesses which still exist in public finances and which, in order to have sustainable policies, should be corrected.

In the communication of the sustainability assessments, these uncertainties could and also should be taken into account in order to have a reliable and sound picture.¹⁴⁰ The National Audit Office of Finland as the fiscal watchdog (Independent Fiscal Institution) in Finland has recommended that specific attention should be paid in the analyses and communication of the structural weaknesses in the economy and not only to a single figure on financial position of the government at a single point of time.¹⁴¹ This is more useful also for policy-making purposes since such analyses allow better focus to the necessary policy actions rather than simpler communications on individual indicators.

The population paths and the adjustment of national economy to different population paths is a significant source of uncertainty in sustainability analyses. In Finland, the ETLA Research Institute of Finnish Economy has produced in research cooperation with the National Audit Office studies on the sustainability of public finances using stochastic assessments. In these studies, uncertainties related to the population growth have been analysed by using stochastic population forecasts. These studies were aimed at developing ways to communicate about uncertainty and to highlight the underlying structural issues and other issues relevant for policy-making.¹⁴² In these

¹³⁹ This is stated in the Governmental Programme itself, see the Programme of the Government of Prime Minister Jyrki Katainen, valtioneuvosto 2011, p.9.

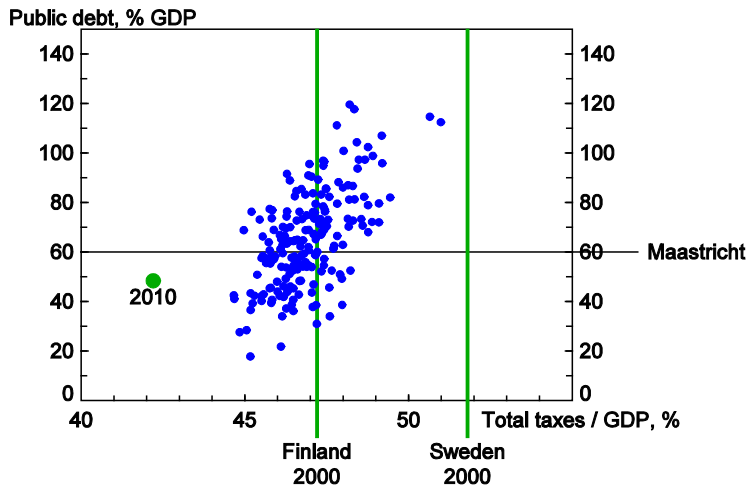
¹⁴⁰ National Audit Office of Finland Special Parliamentary Report: Effectiveness of Expenditure Ceilings in the Governance of Fiscal Policy, The Electoral Period 2007 – 2011 Report on the Fiscal Policy, Parliamentary Reports K 21/2010 vp., see valtionalouden tarkastusvirasto 2011b, p. 180 – 187.

¹⁴¹ National Audit Office of Finland Special Parliamentary Report: Mid-term 2011 – 2014 Review of Fiscal Policy, Parliamentary Report K 2/2013, see valtionalouden tarkastusvirasto 2013d.

¹⁴² See Lassila & Valkonen 2013. Lassila, Valkonen & Alho 2011. Lassila & Valkonen 2011. Lassila & Valkonen 2008. Results of studies will be presented in a forthcoming journal article, see Jukka Lassila, Tarmo Valkonen and Juha M. Alho (2014): Demographic Forecasts and Fiscal Policy Rules. Forthcoming in The International Journal of Forecasting.

studies, the sustainability gap has been expressed with confidence intervals and a presentation based on dot figures corresponding to various probabilities and various possible adjustment paths of the Finnish economy is used.

Figure 1. Public debt and taxes in Finland in 2060



Source: adapted from Jukka Lassila, Tarmo Valkonen and Juha M. Alho (2014): Demographic Forecasts and Fiscal Policy Rules. Forthcoming in *the International Journal of Forecasting*.

Figure 1 is adapted from the studies made by ETLA. In figure 1, blue dots represent different stochastic population scenarios and the combination of the public debt and total tax rate related to the given stochastic population path, derived from a dynamic general equilibrium model. The green dot describes the situation of Finland in 2010. The debt to GDP reference value set by the current Treaty on the Functioning of the European Union, originally agreed in the Maastricht Treaty and the situation of Finland in the year 2000 and Sweden in the same year are also presented. The areas of the figure which have a concentration of blue dots are the most likely outcomes. Sweden has been chosen because of its proximity in terms of its societal values and its economic and societal structures. The comparison with the tax rate also tells, to a certain extent, about the possibilities for tax increases albeit in tax policy also other aspects should be taken into consideration. The aim is, thus, in a graphic way present different stochastic paths and probabilities in an understandable format. The objective of such presentation of the results is, thus, to communicate both the complex realities and the complex calculations of the stochastic sustainability analyses conducted in a dynamic general equilibrium model of the Finnish economy.

The communication of uncertainties and probabilities is a considerable challenge. An argument against the stochastic sustainability analyses is that they are too complex and very difficult to communicate to the general public and, also to the political decision-makers. However, from the communicational rights points of view such analyses and communications include the background information and access to multiple assumptions and knowledge about uncertainties that form the rational public debate perspective the public should be aware of.

The reading of such information and the participation to such discourse, however, sets high demands for intellectual and factual abilities of the participants. It could also be argued that such public communications may only be used and be useful in societies in which the general education level is very high. The role of the media is pivotal as the provider of general information to the public and also to the effectiveness of the independent fiscal institutions.¹⁴³ Newspapers and other institutions of established media are still, even at the age of social media and network based communications, important agenda setters, bringing issues to the national debate and information intermediaries transmitting information to which interested users will then directly dive into. stochastic sustainability analyses and other more complex presentations of the financial situation and options of the fiscal policy require also, then, a well-informed and well-educated cadre of financial and economic journalists and communications markets with sufficient interest to such kind of reporting and information in order to allow such analyses to become really and effectively part of the citizens' political information rights.

Graphics and, in particular information graphics may help in the communication of stochastic analyses and other analyses with more comprehensive information about probabilities and various alternatives. Such communications are also easier to present in computer-assisted communications. There seems to be a trend in mass media to increasingly use animations and computer-created information graphics to present information and communicate them efficiently. Also this seems to be a trend in the presentation of fiscal and financial watchdog bodies' findings. Good examples of this are, among others as good but different kinds of examples, the United States Congressional Budget Office and the Netherland's Court of Audit (Algemene Rekenkamer). The Netherland's Court of Audit has, among other things, created a thematic website with very graphical design to inform citizens about the public interventions to subsidise banks and financial institutions during the crisis between 2008 – 2012.¹⁴⁴ CBO publishes regularly long-term budget reports in which it also discusses the alternative scenarios and uncertainties in projections.¹⁴⁵ The CBO places its most important message as a graphic on the cover-page of its report since busy legislators in the context of contemporary information over-flood are not necessarily reading lengthy reports. The CBO website has not yet any specific animated or interactive information graphics albeit the CBO generally speaking pays a lot of attention to good concise communications about the results of its analytical work.

The presentation of the uncertainties in the fiscal policy is relevant to the information and communication policy and also to constitutional ideals of transparency and democracy in many dimensions. A general argument is that information policy and governmental communications should endeavour to give a fair and truthful presentation of the reality, and, since economic and budgetary forecasts are shaped by assumptions and contain several uncertainties, these should also be presented faithfully and transparently. Another topic is increasingly debated in the academic literature: Leeper argues that transparency seems to be different in monetary policy and fiscal policy. In monetary policy, transparency is a means to the monetary policy ends whereas in fiscal policy transparency relates more to the integrity of the policy-making process itself. In fiscal policy projections are – and according to Leeper – too often silent about possible future fiscal policies. This

¹⁴³ See IMF 2013.

¹⁴⁴ See <http://kredietcrisis.rekenkamer.nl/en/interventies> (page visited 15.12.2013).

¹⁴⁵ See, for example, the CBO 2013 Long Term Budget Outlook, <http://www.cbo.gov/publication/44521> (page visited 15.12.2013). The CBO Long Term Budget Outlook Reports contain also a specific chapter on the analyses of uncertainties but not yet a comprehensive use and regular presentation of stochastic analyses for the whole federal budget. The CBO performs such analyses in its reports on the financial outlook for the Social Security trust funds; see Congressional Budget Office, The 2012 Long-Term Projections for Social Security: Additional Information (October 2012), www.cbo.gov/publication/43648, and Quantifying Uncertainty in the Analysis of Long-Term Social Security Projections (November 2005), www.cbo.gov/publication/17472.

would also improve behavioural impacts and in the long run, effectiveness of fiscal policy. Leeper's analysis focuses not on the democratic or normative aspects of information and communication policy but on the significance of transparency and clear communications to the influencing of economic decisions.¹⁴⁶ According to the Constitution of Finland, the Parliament has the right to receive all information which is necessary for the performance of its duties.¹⁴⁷ Since budgetary and economic forecasts are material for the decision-making on legislation and budgets, the Parliament shall have access to estimations on uncertainties and risks in the forecasts. From the citizens' communicational rights perspective, access to background knowledge on policy alternatives to assess governmental policy choices improves the conditions of democratic choice and debate. The citizens' right to knowledge and effective democratic participation calls upon the production of independent scientific analyses and other expert analyses on the policy alternative and policy uncertainties and to arrive at this access to data on various alternatives should be available.

The European Union Budgetary Frameworks Directive 2011/85/EU exactly requires sensitivity analyses and presentation of supplementary scenarios to the most likely macro-fiscal scenario and the public availability of the methodologies, assumptions and parameters underlying the forecasts and the comparison of the Member States official forecast to those of the Commission and to forecasts prepared by other institutions.¹⁴⁸ The requirement concerns medium-term and short-term macro-economic and budgetary forecasts but the same principle should also be applied to the presentation and communication of long-term sustainability issues.

The discussion on the presentation of financial and economic data leads to the wider question of the use of open data and web-based information and communication portals in the governance policy of today. Governance policy refers here to an explicitly articulated idea on how different regulatory and steering instruments the Government has at its disposal and how they should be used in the endeavour to realise societal policy targets of the government. The European Union Budgetary Frameworks Directive 2011/85/EU bears the inherent policy idea that open data and easy access to economic and budgetary forecasts shall be used to make an impact to public national debate and to public decision-making. Purpose of the Directive is to better-connect the European Semester with the European Steering to the national policy-making discourses. Another objective is to rectify certain information biases, such as unrealistic and too political macroeconomic scenarios and hereby strengthen the incentives and conditions for disciplined fiscal policies with the aim of structural balance and long-term sustainability. The Directive puts in place a normative communication policy on that regard. The Directive's requirements in Article 4 on the access to data and presentation of the forecasts and in Article 3 on statistics and accounting and in Article 14 on the structure of the public sector and extra-budgetary bodies, impact of tax expenditures and contingent liabilities set an agenda of open data driven governance and steering. The Directive, thus, sets legal requirements for communication and information policy related to fiscal policy, fiscal situation and macro-economic and budgetary forecasting.

The issue of the use of open data and information-driven steering is however a wider issue currently at debate in the academia and in practise in several OECD countries. In Finland, both the NAOF and the OECD have recommended a considerably strengthened use of open data and easy to capture information dissemination in the steering and governance of public sector. According to the OECD, in its Public Governance Review of Finland from year 2010, there is a need for the Gov-

¹⁴⁶ Leeper 2009.

<http://www.nber.org/papers/w15269>.

¹⁴⁷ Section 47 of the Constitution of Finland.

¹⁴⁸ See Budgetary Framework Directive 2011/85/EU, preamble para. 9 – 12, Article 4 (1), (4) and (5). The European Commission shall also publish methodologies, assumptions and parameters underlying its macroeconomic and budgetary forecasts, see Article 4 (2) of the Budgetary Framework Directive 2011/85/EU.

ernment to better communicate the difficult challenges and choices the country needs to make. This means, in particular, that long-term costs and benefits of the policy choices and alternatives connected with the long-term fiscal projections shall be made easily available to citizens. In addition, the OECD highlights the Norwegian KOSTRA reporting system on finances and performance of local government as a possible model to step up data collection and analyses as well as communication with citizens and expert communities. According to the OECD, local governments would particularly gain from such increased transparency and unity of data and ease of data collection and dissemination.¹⁴⁹ KOSTRA is a web-based service of Statistical Bureau of Norway reporting on the goals, performance and finances of the Norwegian local government.¹⁵⁰ The National Audit Office of Finland sees steering based on open data and easy access to information, including comparative information, as tools of the so called smart steering and governance in the public sector.¹⁵¹

The presentation of financial and economic information and forecasts and giving access to the underlying background data is not only an issue of communication and information policy: they have wider implications for the constitutionalism. The European Union Budgetary Frameworks Directive 2011/85/EU seems, partly, to represent an example of material constitutionalism and constitutionalisation in which certain substantive requirements for policy-making and underlying information used in the policy making are represented. Constitutionalism has different versions in Europe. There are differences between the rule of law and constitutionalism between Europe and the United States of America which shall be born in mind when comparing governance systems and academic literature on economic governance and information policy. The rule of law in the American context and, also in the English law and constitution, tend to be more formal and focus on fair process in courts whereas in Continental Europe constitutionalism is more state-centred and tends to establish general substantive principles which the constitutional state shall respect and promote.¹⁵² However, the concept of rights, which can be called upon and enforced in the court proceeding also against legislative texts, is very strongly present in the American history and practise, and, since World War II, in the practise of the German Constitutional Court. Constitutionalism can be understood in different ways in the European Union and Member States contexts albeit there has been a significant convergence of constitutionalism and underlying ideas of constitution are historically shared and similar.

The core of the constitutionalism is, historically, in the binding of the state power to law and constitution and giving special weight to a text or practise called the constitution. Today constitutionalism is shaped by the primacy of fundamental rights. Constitutionalism means also giving weight in public functions and activities to the principles and rules defined in the constitution. Constitutionalism leads to a concept of political democracy which emphasises substantive principles and arguments over formalism; in today's constitutionalism, the adherence to and the optimal realisation of the fundamental rights and freedoms form its primal substance.¹⁵³

The Budgetary Frameworks Directive is not a constitutional text but it defines criteria for the exercise of fiscal policy, a key area of political life, and further defines transparency and access-to-

¹⁴⁹ OECD 2010.

¹⁵⁰ See <http://www.ssb.no/offentlig-sektor/kostra> (page visited 15.12.2013).

¹⁵¹ National Audit Office of Finland Annual Report to 2013 Parliamentary Session, Parliamentary Reports K 18/2013 vp., see *valtionalouden tarkastusvirasto 2013b*.

¹⁵² On the difference of formal and procedural rule of law and substantive constitutional state in procedure and role of the courts in democracy, see Garapon & Papadopoulos 2003. Similar distinction can be made also concerning ideas of constitutionalism and information policy.

¹⁵³ See Ferrajoli 2011. Habermas 2001. On the Finnish debate on constitutionalism related to Europe, see, for example, Nieminen L. 2004, Nieminen L. 2010, Ojanen 2009 and Husa 2009. There is a wide literature concerning constitutionalism and its development in the European Union.

information rights related to public policy-making. It can be counted as part of a wider constitution, part of legally binding documents defining the rules of the game of politics and public policy-making and limiting the practises and use of power that the European Union national legislators and national governments may adopt and use. The enactment of the Budgetary Frameworks Directive and its definition of the access to information rights further strengthen substantive constitutionalisation.

The whole concept of the citizens' informational rights represents a fairly strong constitutionalism; information policy and communication policy will increasingly be defined legally and become a constitutional matter. The various faces and nuances of constitutionalism also mean that the significance of the access-to-information rights and communication policy principles in the Budgetary Framework's Directive will be different in various Member States of the European Union. The budgetary Framework Directive also sees the information policy and communicational rights in a teleologic and instrumental way. They are instruments for attaining a disciplined fiscal policy rather than elements of democracy. The information and communication policy in the Budgetary Framework Directive represents an incrementalist approach to decision-making and public sector reform. Incrementalism is one of the critiques of rationalism and it is based on the concept of bounded rationality. Incrementalism sees that models of perfect rationality exaggerate information and knowledge capacities of decision-makers. Therefore in public decision-making small successive improvements shall be made instead of comprehensive reforms and use successive limited comparisons and reforms as a manner to improve public policies, administration or, in budgeting, the efficiency of resources allocations. Incrementalism is, thus, a realistic approach to how public policy-making is limited in practise.¹⁵⁴

6. Conclusions

The new legal rules of economic governance in the European Union represent a further step in a teleological and instrumental constitutionalisation of information policy in the European Union. Transparency is seen as a method of promoting and assuring a disciplined fiscal policy leading to more sustainable public finances than alternative policies.

Despite these critical remarks, the new economic governance rules in the Fiscal Compact and in the Six Pack and Two Pack add a more transparent dimension to the economic policy coordination, that of open public debate of policy alternatives, economic forecasts and assessments of economic policies, and also, significantly increased access to information. This new dimension is added to the classic communication policy of international and inter-governmental peer review behind the closed doors of the Council of the European Union and meetings of the Eurogroup.

In particular, Regulation (EU) 473/2013 and Budgetary Framework Directive 2011/85/EU open up for a deliberative democracy and establish the requirement of open public discourses to the sphere of fiscal policy. From the Finnish perspective, this has the potential for strengthened democracy. The democratic legitimisation of the Stability and Growth Pact is increased if the transparency potential of the new provisions is fully exploited.

The Budgetary Framework Directive establishes new provisions concerning access to data and information in the Member States and sets requirements for the public sector to produce data and make it publicly available. Furthermore, the Directive requires the production of comparative information on the economic scenarios and thereby broadens the analysis presented in the official

¹⁵⁴ On incrementalism in the European Union's own budget and as an approach to budget processes, see Saarihahti 2012, p. 57-61. Classic texts on the budgetary processes and incrementalism are Lindblom 1959, Braybrooke & Lindblom 1963, Wildavsky 1984 (4th edition, 1st edition 1964), Etzioni 1968.

policy discourses. The access rights in the Directive reach to background data, assumptions, methodologies and parameters underlying economic and budgetary forecasts and not only to the economic forecast itself. This new dimensions also concern access to the application which contains the parameters and methodologies for forecasting. This corresponds to the development of the citizens' communicational rights which include rights to background data and to the contextualising data and information.

Access to public sector information and the communication strategies attached to it are not any longer access to a single document. The citizens' communicational rights, in particular right of access to (1) information and knowledge (factual information), (2) to background knowledge concerning social and political choices, (3) to a belonging to a communicational and discursive community and (4) to self-expression and being listened to, systematise constitutional ideals in the European Union which can also be attached to the information and communication policy of the EU's revised rules on economic governance. The right of access to information and knowledge itself is a multi-dimensional and multi-layered right. It contains access to core data and the availability of such data in computer-readable formats. According to the Budgetary Framework Directive this right of access includes the access to parameters, assumptions and methodologies on the basis of which the economic forecasts are done. This creates an additional dimension to the access rights, the right of access to the background data and knowledge making the information understandable. The Directive stipulates specific information production obligations for the Member States authorities and also requires the assurance of the quality of information. All this can also be seen as elements supporting the ideals of enlightened public debate.

The Fiscal Compact, Budgetary Framework Directive and Regulation (EU) No 473/2013 and the Fiscal Compact require functionally independent oversight bodies, independent fiscal institutions, sometimes referred to as fiscal councils, to participate as active participants to the public discourses on fiscal policies. The Communication on the common principles and the Regulation (EU) No. 473/2013 stipulate that the Independent Fiscal Institutions shall have unlimited access to communicate the results of their work in public. The reason for this is teleological, but this also induces the activation of public discourses and broadens them in the spirit of the ideals of an enlightened public debate.

The IMF has concluded in the analysis of the effectiveness of the independent fiscal institutions that their impact on the fiscal discipline and sustainability of fiscal public finances depends on their capacity of communication in the public. This highlights the significance of the public debate and discourses on the long-term sustainability and fiscal discipline. Public discourses are also a way to transmit steering messages of fiscal policy and hereby anchor them in the decision-making process of citizens, companies and other economic actors.

Good information and communication are a way to remedy fiscal illusions which contribute to in the long run less than rational fiscal policy. Ideals of democratic deliberation and of disciplined fiscal policy hereby concur. The deliberative enlightened public debate can promote fiscal discipline and sustainability of fiscal policies. The citizens' communicational rights and the rights of access to information which are part of these communicational rights, are at the centre of the reconciling between the sustainability of fiscal policies in the longer term and democratic ideals. The principles of good administration and good government shall thus be strengthened as part of the measures to overcome the economic and financial crisis and constitutional crisis the European Union currently faces. The realisation of communicational rights and enlightened public debate at the Member States medias and arenas on European economic and fiscal policy topics, based on high quality information and a description of the full variety of economic phenomena and governmental actions, is a way to bring back citizens into the political debate and strengthen the legitimacy in the transnational intergovernmental co-operation of which the economic governance in the European

Union is a primary example. This is an important communication and information policy goal albeit it is difficult to realise in practise.

The future is uncertain. The future is unknown. The communication of a fair view of the macro-economic forecasts of the sustainability analyses and policy alternatives requires information and communication about uncertainties and various scenarios. Economic actors modify their action on the basis of new information and changing situation. This means that analyses solely based on the continuation of the unchanged policy does not sufficiently describe the future albeit it is also important to show the scenarios based on unchanged policy conditions. Similarly to give sufficient background information and access to contextualised knowledge about the risks presentation of different scenarios and sensitivity analyses. However, the communication of such kind of analyses requires specific considerations for the audience and their capacity to assess and understand information. Informed citizenship can be seen as the underlying democratic ideal in the new economics related information policy of the Union albeit the point of departure of the regulation is an incrementalist rectification of the biases in fiscal decision-making.

The ideals of enlightened public debate set very high demands for the participants. Research has shown that background knowledge shapes considerably how people understand and react to economic information and which kind of consequences they draw on the information provided. The quality of the ensued public debate and also the effectiveness of the Independent Fiscal Institutions depend on the functioning and quality of media and journalism. This also creates conditions for the Independent Fiscal Institutions to achieve the goals the new EU economic governance rules set for them. The opening up of the background of calculations and policy alternatives is, nevertheless, important for the material functioning of democracy so that policy-makers can have authentic alternatives and understanding of the consequences of various decisions and to have understanding of the significance of the key indicators informing or even determining the content of fiscal and economic policies. This is very important when indicators such as structural balance, which is a theoretic indicator and cannot be observed, but, rather, is based on fairly complicated calculations, is used as key indicators steering public policy-making.

Information graphics and computer-based illustrations and animations may provide powerful tools to communicate efficiently complex and technical realities. They can also be used to communicate stochastic analyses and highlight probabilities. The use of such information graphics can be considered to be in line with the citizens' communicational rights providing the constitutional ideals for communicating about economic policy. Then however, the general public shall have access to the assumptions and methodologies underlying graphics and illustrations.

My analyses of citizens' informational and communicational rights and discussion about deliberative democracy is here limited to one specific field; the European Union economic governance. Analyses show that very interesting legal developments take place in the field of special legislation. Some core areas of government data, statistical data and public accounting data among others, are subject to special legislation which contains exceptions or different regulatory solutions than the general freedom of information legislation. Quite often specific sectors of law are areas of very significant legal and policy developments. Such specific developments sometimes escape from the attention of scholars.

Reforms of economic governance induce changes in governmentality and in the ideas concerning governmentality. Change in governmentality is partly intentional and partly result of unconscious and unintentional and cultural developments. The European Union is not a uniform system of governance and thereby reforms bring in several and even conflicting ideas of governance and governmentality. Albeit some of them may enjoy a dominant position some others are embedded in the elements and compromises present. Deep structures of governmentality never represent a one and universal truth and pattern but several conflicting ideals and struggles. The most noticeable

current in the gradual but still rapid changes in governmentability is the transition from a community of liberal nation states with state administrations towards universal and transnational knowledge of experts in which the ultimate impact of knowledge rather than liberal participation provides legitimacy. Changes imply mathematisation of governance and knowledge leading easily to less transparent decision-making. The presentation of uncertainties, various scenarios and adjustments path and the underlying assumptions is also a counter-measure to the mathematisation of knowledge.

Methodologically, critical constructivism provides interesting angles to the analysis of information policy and information law. In the future research, joint analyses combining law, economic and information policy studies would be a promising way to approach several of the core questions in the changing governance, in the special field of economic policy and also in the analyses of governmental information policies in general. Critical constructivism can help to develop legal systematics and assessments of information and communication policy for the legitimacy, a core constitutional value.

7. References

[Acemoglu, Egorov & Sonin 2013]

Acemoglu Daron , Egorov Georgy and Sonin Konstantin: A Political Theory of Populism. *The Quarterly Journal of Economics* (2013), p. 771 – 805.

[Akerlof & Schiller 2009]

Akerlof G.A. and Schiller R.J.: *Animal Spirits: How Human Psychology Drives the Economy, and Why It Matters for Global Capitalism*. Princeton University Press, Princeton 2009.

[Alesina & Cukierman 1990]

Alesina Alberto and Cukierman Alex: The Politics of Ambiguity. *The Quarterly Journal of Economics*, Vol. CV (1990), p. 829 – 850.

[Alessina, Ardagna & Trebbi 2006]

Alessina Alberto , Ardagna Silvia and Trebbi Francesco: Who adjusts and When? The Political Economy of Reforms. *IMF Staff Papers*, Vol. 53, Special Issue. IMF 2006.

[Alesina & Tabellini 2007]

Alesina Alberto and Tabellini Guido: Bureaucrats or Politicians? Part I: A Single Policy Task. *The American Economic Review*, Vol. 97 (2007), 169 – 179.

[Bi & Leeper 2013]

Bi Huixin and Leeper Eric M.: *Analyzing Fiscal Sustainability*. Bank of Canada Working Paper 2013-27, Bank of Canada 2013.

[Bi, Leeper & Leith 2013]

Bi Huixin, Leeper Eric M. & Leith Campbell: Uncertain Fiscal Consolidations. *Economic Journal*, Royal Economic Society, Vol. 123 (2013), p. F31-F63.

[Boscheck 2006]

Boscheck Ralf: EU Constitutional Governance: Failure as Opportunity. *Intereconomics*, January/February 2006, p. 25 – 36, p. 30.

[Braman 2006]

Braman Sandra: *Change of state: Information, policy and power*, Cambridge MA, MIT Press 2006.

[Braman 2008]

Braman Sandra: Policy Research in an Evidence-Averse Environment. *International Journal of Communication*, Vol. 2 (2008), 433 – 449.

[Braman 2011]

Braman Sandra: Defining Information Policy. *Journal of Information Policy*, Vol. 1 (2011), p. 1-5, p. 3.

[Braman 2011b]

Braman Sandra: The Representational Economy and the Global Information Policy Regime, in Albagli Sarita and Maciel Maria Lucia (eds.): *Information, Power and Politics: New Technological and Institutional Mediations*. Boulder, CO: Lexington Books 2011, p. 27 – 46.

[Braybrooke & Lindblom 1963]

Braybrooke David & Lindblom, Charles E.: *A Strategy of Decision: Policy Evaluation as a Social Process*. The Free Press. Glencoe, Illinois 1963.

[Bräutigam 2008]

Bräutigam Tobias: Bräutigam, Tobias: *Rechtsvergleichung als Konfliktvergleich : das deutsche Informationsfreiheitsgesetz aus Perspektive des US-amerikanischen und finnischen Rechts*, University of Helsinki Dissertations, Helsingin yliopisto 2008.

[Calmfors 2005]

Calmfors Lars: What Remains of the Stability and Growth Pact and What Next?, SIEPS Report No 8. Swedish Institute for European Policy Studies, Stockholm 2005.

[COM (2008) 229 final]

European Commission: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL regarding public access to European Parliament, Council and Commission documents, COM (2008) 229 final, COD 2008/90.

[COM (2010) 523 final]

European Commission: Proposal for a COUNCIL DIRECTIVE on requirements for budgetary frameworks of the Member States, COM (2010) 523 final, 2010/277 (NLE).

[COM (2011) 877 final]

European Commission: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL Amending Directive 2003/98/EC on re-use of public sector information, COM (2011) 877 final, COD 2011/430.

[COM (2013) 114 final]

European Commission: REPORT FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT, Towards implementing harmonised public sector accounting standards in Member States. The suitability of IPSAS for the Member States {SWD(2013) 57 final}. COM (2013) 114 final.

[Council of Europe 2013]

Council of Europe, Commissioner for Human Rights: *Safeguarding human rights in times of economic crisis*, Issue Paper 2013. Council of Europe 2013.

[Debrun, Hauner & Kumar 2009]

Debrun Xavier, Hauner David and Kumar Manmohan S: Independent Fiscal Agencies. *Journal of Economic Surveys*, 23:1 (2009), p. 44-81.

[Dobson 2012]

Dobson Andrew: Listening: The New Democratic Deficit. *Political Studies*, Vol. 60 (2012), p. 843 – 859.

[Earle 2009]

Earle T.C. : Trust, Confidence and the 2008 Global Financial Crisis. *Risk Analyses* 29 (2009), pp. 785 – 792.

Etzioni Amitai: *The Active Society. A Theory of Societal and Political Processes*. The Free Press. Collier-MacMillan Limited, New York 1968.

[European Commission 2012]

European Commission: *Fiscal Sustainability Report 2012*. *European Economy* 8/2012.

[European Commission 2013a.]

European Commission: *Building a Strengthened Fiscal Framework in the European Union: A Guide to the Stability and Growth Pact*. *European Economy, Occasional Papers* 150, 2013.

[European Commission 2013 b.]

European Commission: *Vade mecum on the Stability and Growth Pact*. *European Economy, Occasional Papers* 151, 2013.

[Fatas & Mihov 2003]

Fatas, Antonio and Mihov, Ilian: The case for restricting fiscal policy discretion. *Quarterly Journal of Economics*, Vol.118(4) (2003), p.1419 – 1449.

[Ferrajoli 2011]

Ferrajoli Luigi: *The Normative Paradigm of Constitutional Democracy*, *Res Publica* Vol. 17 (2011), p. 355–367.

[Frankel & Schreger 2013]

Frankel Jeffrey A. and Schreger Jesse: Over-optimistic Official Forecasts and Fiscal Rules in the Eurozone. *Review of World Economics*, Vol. 149 (2013), p. 247-272.

[Gangl et. al. 2012]

Katharina Gangl, Barbara Kastlunger, Erich Kirchler and Martin Voracek: Confidence in the economy in times of crisis: Social representations of experts and laypeople. *The Journal of Socio-Economics* 41 (2012), 603 – 614.

[Garapon & Papadopoulos 2003]

Garapon, Antoine – Papadopoulos, Ioannis: *Juger en Amérique et en France: Culture juridique française et common law*. Paris: Odile Jacob, 2003.

[Gosh et. al. 2013]

Ghosh Atish R., Kim Jun I., Mendoza Enrique G., Ostry Jonathan D. and Qureshi Mahvash S.: Fiscal Fatigue, Fiscal Space and Debt Sustainability in Advanced Economies. *Economic Journal*, Vol. 123 (2013), p. F4-F30.

[Grant & Keohane 2005]

Grant Ruth W. and Keohane: Robert O.: Accountability and Abuses of Power in World Politics. *American Political Science Review*, Vol. 99 No. 1 (2005), p. 29 – 43.

[Haaparanta 2011]

Haaparanta Pertti: *Julkisen talouden kestävyyslaskelmista*. *Kansantaloudellinen aikakauskirja*, Vol. 107 (2011), p. 59 – 75.

[Habermas 1998]

Habermas Jürgen: *Faktizität und Geltung. Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*, Frankfurt am Main, Suhrkamp, 1998.

[Habermas 2001]

Habermas Jürgen: Constitutional Democracy: A Paradoxical Union of Contradictory Principles? *Political Theory*, Vol. 29 (2001), p. 766 – 781.

[Habermas 2003]

Habermas Jürgen: On Law and Disagreement. Some Comments on “Interpretative Pluralism”. *Ratio Juris*, Vol. 16 No. 2 (2003), p. 183 – 194.

[Habermas 2012a]

Habermas Jürgen: The Crisis of the European Union in the Light of a Constitutionalization of International Law, *The European Journal of International Law* Vol. 23 no. 2 (2012), p. 335–348.

[Habermas 2012b]

Habermas Jürgen: Bringing the Integration of Citizens into Line with the Integration of States. *European Law Journal* Vol. 18, No. 4, July 2012, p. 485–488.

[Hallerberg, Strauch & von Hagen 2007]

Hallerberg M., Strauch R. and von Hagen J.: The Design of Fiscal Rules and Forms of Governance in European Union Countries. *European Journal of Political Economy* 23 (2007), 338–359.

[Hillman 2004]

Hillman A: Corruption and Public Finances. An IMF Perspective. *European Journal of Political Economy* 20 (2004), p. 1067–1077.

[Husa 2009]

Husa Jaakko: Konstitutionalismin mahdollisuus? *Lakimies* 2009, 1141 - 1153.

[Ilmakunnas 2012]

Ilmakunnas Seija: Eurokriisi, finanssipolitiikan uudet säännöt ja Suomi. *Talous ja yhteiskunta* 4/2012, p. 28 – 34.

[IMF 2013]

International Monetary Fund: The Functions and Impact of Fiscal Councils. IMF Policy Paper, 16.7.2013.

[Kahneman & Tversky 1979]

Kahneman D. and Tversky A.: Prospect Theory: An Analyses of Decision under Risk. *Econometrica*, Vol. 47 (1979), p. 263-291.

[Kahneman & Tversky 1984]

Kahneman D. and Tversky A.: Choices, Values and Frames. *American Psychologist*, Vol. 34 (1984), reprinted in Daniel Kahneman: *Thinking Fast and Slow*, Penguin Books 2011, p. 433-448.

[Kauffman & Vicente 2011]

Kauffman D ja Vicente P.C.: Legal Corruption. *Economics and Politics* (2011), Vol. 23., p. 195–219.

[Korkman 2010]

Korkman Sixten: Finanssipolitiikan instituutiot ja julkisen talouden rahoituksen kestävyys, in Valtioneuvoston kanslia: Finanssipolitiikan instituutiot, valtioneuvoston kanslian julkaisusarja 18/2010, p. 33 - 64. p. 37-42.

[Lassila & Valkonen 2013]

Lassila, Jukka & Valkonen, Tarmo (2013): *Julkisen talouden rahoituksellinen kestävyys*, ETLA Raportit, No 3, 2013.

[Lassila & Valkonen 2011]

Lassila, Jukka - Valkonen, Tarmo (2011): Julkisen talouden rahoituksellinen kestävyys Suomessa 2011, ETLA Keskusteluaiheita nro 1237.

[Lassila & Valkonen 2008]

Lassila, Jukka & Valkonen, Tarmo (2008): Fiscal Sustainability in Finland: a stochastic analysis, Bank of Finland Research Discussion papers 28/2008.

[Lassila, Valkonen & Alho 2011]

Lassila Jukka, Valkonen Tarmo and Alho Juha M (2011): Fiscal Sustainability and Policy Rules under Changing Demographic Forecasts, ETLA Keskusteluaiheita / Discussion papers No 1265, ETLA 2011.

[Leeper 2013]

Leeper, Eric M.: Fiscal Limits and Monetary Policy. Central Bank Review, Research and Monetary Policy Department, Central Bank of the Republic of Turkey, vol. 13(2) (2013), p. 33-58.

[Leeper 2009]

Leeper Eric M: Anchoring Fiscal Expectations. Reserve Bank of New Zealand Bulletin, Reserve Bank of New Zealand, Vol. 72 (2009), 17-42.

[Leino-Sandberg & Salminen 2013]

Leino-Sandberg Päivi and Salminen Janne: Eurokriisin demokratiaulottuvuuksia, Lakimies 2013 (3), p. 390 - 413.

[Lindblom 1959]

Lindblom Charles E: The Science of "Muddling Trough", PAR Vol. 19 (1959):2, p. 79 -88.

[Marzilli Ericson & Fuster 2011]

Marzilli Ericson Keith M. and Fuster Andreas: Expectations as endowments: evidence on reference-dependent preferences from exchange and valuation experiments. Quarterly Journal of Economics, (2011) Vol. 126, p. 1879 – 1907.

[Mauro 1995]

Mauro P.: Corruption and Growth. Quarterly Journal of Economics 110 (1995), 681–712.

[McGuire 2011]

McGuire Chad: A Framework for Analyzing Information Flows in Public Policy Decision-making: A Move towards Building Sustainable Policy Instruments. Journal of Politics and Law, Vol. 4 (2) (2011), p. 25 – 35.

[Méndez & Sepúlveda 2006]

Méndez F. and Sepúlveda F. Corruption, Growth and Political Regimes. Cross Country Evidence. European Journal of Political Economy 22 (2006), p. 82–98.

[Mäenpää 2013]

Mäenpää Olli: Hallinto-oikeus, SanomaPro, Helsinki 2013.

[Nieminen 2007]

Nieminen Hannu: Median sääntely ja informoitu kansalaisuus, in Satu Paasilehto (ed.): Demokratia ja säädöspolitiikka. Eduskunnan juhlaseminaari 2. lokakuuta 2006, Eduskunnan kanslian julkaisu 1/2007, Eduskunta, Helsinki (2007), p. 59-70.

[Nieminen L. 2004]

Nieminen Liisa: Eurooppalaistuva valtiosääntöoikeus – valtiosääntöistytvä Eurooppa, Suomalainen lakimiesyhdistys, Helsinki 2004.

[Nieminen L. 2010]

Nieminen Liisa: Eurooppalainen konstitutionalismi, Lakimies 2010, p. 773-790.

[OECD 2002]

OECD Best Practise for Budget Transparency. OECD, Paris 2002.

[OECD 2010]

OECD: Finland: Working Together to Sustain Success, OECD Public Governance Reviews, OECD Publishing, OECD 2010.

[OECD 2013]

OECD Principles for Independent Fiscal Institutions. OECD Public Governance Committee document GOV/PGC(2013)9/REV1, OECD 2013.

[OECD/Barnes, Davisson and Rawdanowich 2012]

OECD Economics Department/ Sebastian Barnes, David Davidsson and Łukasz Rawdanowicz: Europe's New Fiscal Rules. OECD Economics Department Working Paper No 972. ECO/WKP(2012)49, OECD 2012.

Oikeusministeriö

Säädösvalmistelun prosessimalli, <http://lainvalmistelu.finlex.fi/> (page visited 3.12.2013),

[Ojanen 2009]

Ojanen Tuomas: Perus- ja ihmisoikeudet - eurooppalaisen konstitutionalismin Akilleen kantapää, Lakimies 2009, p. 1106-1124.

[Pöysti 2002]

Pöysti Tuomas: Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet, teoksessa Heikki Kulla ym.: Viestintäoikeus, WSOY Lakitieto, Helsinki 2002, s. 35-81.

[Pöysti 2004]

Pöysti Tuomas: ICT and Legal Principles: Sources and Paradigm of Information Law in IT Law, ed. by Peter Wahlgren, Scandinavian Studies in Law, Vol. 47 (2004), Stockholm Institute of Scandinavian Law, Stockholm 2004, p. 559-600.

[Pöysti 2007]

Pöysti Tuomas: Scandinavian Idea of Informational Fairness in Law – Encounters of Scandinavian and European Freedom of Information and Copyright Law teoksessa Peter Wahlgren (ed.) What is Scandinavian Law? Social Private Law, Scandinavian Studies in Law, Vol. 50, Stockholm University 2007, p. 222 – 248.

[Pöysti 2013]

Pöysti Tuomas: Tilivelvollisuus ja hyvä hallinto, Euroopan uudet haasteet, teoksessa Ala-Nissilä Olavi: Musta aukko – teesejä Brysselin ja Wall Streetin seinille, KHT Media 2013, p. 65 – 81.

[Roland-Lévy, Pappalardo Bourmelki & Guillet 2010]

Roland-Lévy Christine, Pappalardo Bourmelki Fatima-Ezzahra & Guillet Emilie: Presentation of the Financial Crisis, Effect on Social Representations of Savings and Credit. The Journal of Socio-Economics, Vol. 39 (2010), p. 142 – 149.

[Saarilahti 2012]

Saarilahti Ilkka: Euroopan unionin taloushallintojärjestelmän joustavuus. Finanssihallinnollisia tutkimuksia joustavuuden eri muodoista ja kehityksestä vuosina 1968 – 2009, European Press Academic Publishing, Florence 2012.

[Sailas 2013]

Sailas Raimo: Perustuslakimme taipuu eurokriisin kenttäoikeudessa. Kanava 1/2013, p. 30 – 31.

[Suomen Pankki 2013]

Suomen Pankki: Talouden näkymät, Euro & talous 5/2013.

[Tuori 2007]

Tuori Kaarlo: Oikeuden ratio ja voluntas. WSOYpro, Helsinki 2007.

[Tuori 2009]

Tuori Kaarlo: Legitimacy. In The Philosophy of Law: An Encyclopedia. Garland Publishing 1999, p. 493–495.

[Tuori & Tuori 2014]

Tuori Kaarlo & Tuori Klaus: The Eurozone Crisis, A Constitutional Analyses. Cambridge University Press 2014.

[Valtioneuvosto 2013]

Valtioneuvoston periaatepäätös valtion tutkimuslaitosten ja tutkimusrahoituksen kokonaisuudistukseksi, 5.9.2013.

[Valtioneuvosto 2011]

Valtioneuvoston tiedonanto Eduskunnalle 22.6.2011 nimitetyn pääministeri Jyrki Kataisen hallituksen ohjelmasta, VNT 2/2011 vp.

[Valtioneuvoston kanslia 7/2011]

Valtioneuvoston kanslia: Hallituspolitiikan johtaminen 2010 –luvulla, Tehokkaamman strategisen työskentelyn välineitä. Hallitusohjelman seurannan kehittämishanke Kokka. Valtioneuvoston kanslian julkaisu, valtioneuvoston kanslian julkaisusarja 7/2011.

[Valtioneuvoston kanslia 8/2011]

valtioneuvoston kanslia: Poliittisen päätöksenteon tietopohjan parantaminen – tavoitteet todeksi. Poliittikkatoimien vaikuttavuusarvioinnin kehittämisryhmän raportti, valtioneuvoston kanslian julkaisusarja 8/2011.

[Valtiontalouden tarkastusvirasto 2011]

Valtiontalouden tarkastusvirasto: Finanssipolitiikan tarkastusohje. Valtiontalouden tarkastusviraston tarkastusohjeita, valtiontalouden tarkastusvirasto, Helsinki 2011

[Valtiontalouden tarkastusvirasto 2011b]

valtiontalouden tarkastusviraston erilliskertomus eduskunnalle: Valtiontalouden kehysmenettelyn vaikuttavuus finanssipolitiikan hallintavälineenä, finanssipolitiikan tarkastuksen vaalikausiraportti 2007 – 2010, K 21/2010 vp.

[Valtiontalouden tarkastusvirasto 2012]

Valtiontalouden tarkastusviraston erilliskertomus eduskunnalle valtion vuoden 2011 tilinpäätöksen ja tilinpäätöskertomuksen tarkastuksesta, K 14/2012 vp.

[Valtiontalouden tarkastusvirasto 2013a]

Valtiontalouden tarkastusviraston tilinpäätös 2012, toimintakertomus, valtiontalouden tarkastusvirasto 2013, saatavilla <http://www.vtv.fi> -> Tilinpäätökset.

[Valtiontalouden tarkastusvirasto 2013b]

Valtiontalouden tarkastusviraston kertomus toiminnastaan eduskunnalle 2013 valtiopäiville, K 18/2013 vp.

[Valtiontalouden tarkastusvirasto 2013c]

Valtiontalouden tarkastusvirasto: Rakenteellisen jäämän laskennan tarkastus, finanssipolitiikan tarkastus, tarkastuskertomus 13/2013.

[Valtiontalouden tarkastusvirasto 2013d]

valtiontalouden tarkastusviraston erilliskertomus eduskunnalle: Finanssipolitiikan tarkastuksen vaalikauden 2011 – 2014 puoliväliraportti, K 2/2013 vp.

[Valtiovarainministeriö 2013]

Valtiovarainministeriö: Budjettikehysdirektiivin ja budjettisuunnitelmien ennakkovalvonta-asetuksen kansallinen täytäntöönpano, valtiovarainministeriö 29/2013.

[Valtiovarainministeriö 2013b]

Valtiovarainministeriö: Taloudellinen katsaus. Kevät 2013. Valtiovarainministeriö 8a/2013.

[Velasco 2000]

Velasco A.: Debt and deficits with fragmented fiscal policymaking. *Journal of Public Economics*, 76 (2000), 105 – 125.

[von Hagen 2002a]

von Hagen Jürgen: Fiscal rules, fiscal institutions, and fiscal performance. *The Economic and Social Review*, 33 (3) (2002), p. 263–284.

[von Hagen 2002b]

von Hagen Jürgen: Budgeting procedures and fiscal performance in the European communities. *European economy – Economic Papers*, 96 (2002).

[von Hagen & Wolff 2006]

von Hagen Jürgen & Wolff Guntram B.: What do deficits tell us about debt? Empirical evidence on creative accounting with fiscal rules in the EU. *Journal of Banking & Finance*, Volume 30, Issue 12, December 2006, p. 3259–3279.

[Wiberg 2013]

Wiberg Matti: Deliberaatiot ovat manipuloitavissa, strategisia näkökohtia. *Politiikka* 55:2 (2013), p. 98 – 108.

[Wildawsky 1984]

Wildawsky Aaron: *The Politics of Budgetary Process*, first edition 1964, fourth edition, Little, Brown and Company, Boston 1984.

THE MANAGEMENT OF LEGAL DOCUMENTS IN THE SERVICE OF THE RULE OF LAW

Patricia Reyes

Professor on the Faculty of Law of the Universidad de Valparaíso and Head of Legal Resources of the Library of the National Congress of Chile. Blanco 1781, Valparaíso, Chile.
preyes@bcn.cl

Keywords: *Legal information services, legal information resources, open data, interoperability, legal documents, information management*

Abstract: *Legal security and the guarantee of individual rights are key elements for the rule of law. They provide assurance to the citizenry not only through the enforcement of legal norms by the respective organisms, but also with regard to the content and validity of the norms themselves. Furthermore, efficacious relationships between the disciplines that study the law, technologies, and information are indispensable to the design, development, and maintenance of free, open, interoperable, and universal legal document services that provide access to legislative, parliamentary, jurisdictional, and administrative documents. This paper presents a perspective that focuses on the roles of document management and the right to information as means to meet the challenges facing modern democratic societies. It examines the main content and functional relations that information services must adopt.*

1. Introduction

It is clear that the Internet has penetrated deeply into our lives. Today the value of knowledge is overtaking the value of capital as the main factor driving the generation of wealth. We encounter the positive and negative effects of the new information and communication technologies in every aspect of our daily lives. As a result of the emergence of this new culture, it is necessary to build an infrastructure that creates opportunities for all citizens and reduces the digital gap. Moreover, information must be recognized as a basic social commodity that should be made available to every member of society. Only in this way can we give legal efficacy to a fundamental human right: the right to information.

However, for the effective exercise of this right, it is not enough merely to make information available: the information itself must meet standards of integrity, sufficiency, accuracy, timeliness, and relevance, as it is widely recognized that the value of information depends on the quality, precision, and the timeliness of its delivery.

With specific reference to legal information and legislative information, these conditions are latent concerns for the rule of law, which must comply with the principles of security and legal certainty, since knowing the content of the legal norms and their just enforcement are requirements imposed on all democratic legal systems.

To attain this objective with greater efficacy, it is critical for there to be a convergence of the disciplines that study law, technologies, and information.

The research carried out in these disciplines has formed the basis for the development of modern electronic management services based on open, interoperable information. These services share

information through single operations, without duplication, that permit the reuse and improvement of related processes. They are based, inter alia, on free and universal access, the openness of data, the universality of the Web as an informational space, and the emergence of technologies and global standards that exchange and link documents.

In a practical sense, the Library of Congress of Chile has adopted and applied these concepts to provide the general citizenry and the parliament, in particular, integrated access to legal information from various legal sources in the country.

2. Information, technologies, and law in the network society

Today we live and work in a digital environment in which we make extensive use of information networks. The term “network society,” coined by Jan van Dijk in his book *De Netwerkmaatschappij* (1991), accurately describes this new environment, where social networks often constitute the main form of organisation and shape the most important structures of modern society at the individual, organisational, and social levels (Reyes, 2011).

In the context of a network society, according to the research of the Finnish professor Athi Saarenpää (2012), the relationship between law, technologies, and information is fundamental for the construction of a new legal culture under the rule of law. Within the scope of this relationship we can identify the following fundamental elements:

2.1. The Right to information

In the network society it is widely agreed that a well-informed citizenry is a fundamental component of a representative democracy. An informed citizenry is a prerequisite for ensuring that qualified people are elected as representatives and plays a crucial role in monitoring governmental oversight. A well informed public generates greater citizen participation, which, in turn, strengthens innovation, collaboration, and competitiveness.

The right to access public information, which forms part of the general right to information, has been recognized as a fundamental right in numerous international instruments and has been incorporated as such in a majority of the national legal codes over the past few years (Reyes, 2013). This legal codification is essential to ensure that information is in the public domain and available to all citizens. In virtue of this right, citizens not only expect access to the information, they expect the information to be reliable, consistent, current, easy-to-use, easy-to-understand, and, especially, reusable and redistributable.

From this perspective, the right to access information is likewise a right to use that information, since it should permit people to make constructive use of that information under the concepts of transparency, participation, collaboration, and innovation.

Openness of public information is indispensable to achieve this and move from secrecy to transparency as a standard practice, thereby shifting power to the citizenry and democratizing the information.

2.2. Management of legal documents

Legal documents, which have become increasingly abundant and lengthy, require efficacious organisation and processing that allow them to be located and retrieved in an efficient manner. As mentioned, the quality, timeliness, and accuracy of legal information is indispensable for the proper development of social and legal life under the rule of law.

Producing, storing, selecting, and even publishing legal information has traditionally been seen as a technical problem of little interest to researchers of the law. Information, even though it forms the basis for all decision-making, was viewed as pertaining to other disciplines. However, without information, legal work, whether it be legislative, judicial, or academic in nature, cannot take place; for example, how can a modification be made to a legal norm if there is no valid current text of the norm in question? The point is that legal information is a fundamental tool in the daily work of a legislator, a judge, or a professor of law.

Likewise it should be evident that legal information is not principally for lawyers, even though legal theory might suggest so. Legal information has been and is valuable to all sectors of the society. In terms of individual rights, it is legal information that regulates our behaviour in society and, hence, is more important than most of the other information we receive. In this regard there must be a latent concern in all rule of law, expressed under the principles of security and legal certainty, to know the content and the outcome of the enforcement of the law.

In our society there has not been enough emphasis placed on legal certainty. It takes an experienced researcher or jurist to be able to access and retrieve certain legal texts, and even greater expertise to ensure its validity (for example, to determine if it has been tacitly or organically repealed). While some public organisms have complied with the requirement of making this information available in the form of digital documents, this is not sufficient, since general information is often stored in systems that do not have the capability of providing access and retrieval in the future, let alone of integrating related legal information.

Thus, it is abundantly clear that the storage, processing, search, and retrieval systems of legal documents must be improved in order to achieve not only the development of the science of law, but also to sustain social solidarity in a democratic society with full efficacy and respect for the fundamental rights.

2.3. Information security

It is also clear that we encounter numerous technological and legal risks in the area of information. In our network society, we no longer live in a world of fixed equipment or connections, but rather have a large part of our information in the cloud. Moreover, transborder relations and the surveillance of data transmission have become a part of daily life. At this point in time, the full extent of the eventual risks is varied and difficult to identify.

Given this scenario, according to professor Saarenpää (2011) we must remember the importance of a key element of the relationship between the law, the technologies, and information: information security. It becomes a crucial factor, even an essential component in protecting individual rights under the rule of law.

If we consider an information system that stores the legal information of a country, protecting that information is essential if we are to provide security and legal certainty to the citizens.

Nevertheless, frequently the information security of these systems is handed over to the technical personnel, who are paradoxically dealing with the rights of millions of citizens without knowing the content and significance of those rights.

Hence, it is imperative that we adopt the necessary security measures for the various systems of legal documentation, bearing in mind the complexity and importance of the information that is stored by our legal culture.

3. The digital environment for the management of legal documents

The area of legal documentation has played a role in the development of information systems. In this regard, today there are certain basic principles and standards that use information and communications technologies to support the management and processing of legal information. In effect, the management of legal documents in a network society must be orientated to the following principles:

3.1. Universal access

Everybody should be able to access official legal information, which consists of legal and parliamentary documents (laws, bills, legal history, session transcripts), jurisdictional information (court rulings), and administrative information (decisions of legal bodies).

3.2. Free of charge

This is a fundamental principle given that it democratises information and prevents cost from becoming a barrier to access. This idea was accepted early on in Europe and was based on the recommendation of the European Council, regarding the need to design and develop legal databases. The general trend toward open and free access to legislative information in Europe and the world started in 1998. The implementation modality was different in every country. Examples of this are: LegiFrance (France), UK Legislation (the UK), Boletín Oficial Español (Spain), Finlex (Finland), Lagrummet (Sweden), LexML (Brazil), and LeyChile (Chile).

3.3. Open data

The movement toward open data rapidly spread throughout the world, starting in 2007, with attempts to create greater awareness of the importance of making information available and to incentivise this process, so that information could be used, reused, and redistributed by citizens.

In subsequent conceptualisations, the concept of open data referred to a veritable philosophy or doctrine based on the "democratisation of information," which declared that information should be accessible, reliable, consistent, current, easy-to-use, and easy-to-understand, but should also be reusable and redistributable. In this sense it is incumbent on governmental institutions to observe the Eight Principles of Open Government Data developed by the working group in Sebastopol, California (2007), which have become the starting point for assessing openness in the management of legal documents.

3.4. Interoperability

In accordance with Decision 387 of the European Community (2004), interoperability is the ability of the systems of information and communications technologies (ICT), and of the business processes supporting them, to exchange information and enable the sharing of information and knowledge.

Being a system of legal information refers to the ability of the system to retrieve information from its own system and from any of the other integrated systems, based on the connectivity established among the content.

Achieving this requires the adherence to common standards, with a multi-layered architecture that resolves and specifies: standardized points of contact; organisational interoperability that coordinates and aligns business processes and information from many institutions; semantic interoperability that ensures common understanding of the meaning of each component in the

exchange process; and technical interoperability, that is, incorporating the technological components compatible with the model of the adopted interoperability.

In the area of interoperability, the following standards proposed and/or implemented by the World Wide Web Consortium (W3C) are fundamental to the development of integrated systems for the exchange of information:

- a. XML (Extensible Markup Language), a type of markup language that functions as a system of information description. It has been chosen as the global standard for processing electronic documents. In simple terms, it is a set of rules that establish semantic protocols that can be applied to the organisation of documents. With XML it is possible to establish a standardized structure for types of documents and to define common metadata that subsequently relate different content.
- b. Web services that refer to a set of protocols and standards that exchange information between applications. These services operate independently of the properties or the platforms on which the applications are installed. They promote standards and protocols based on text, which makes it easier to access content and understand the way it functions. And, by supporting HTTP, they take advantage of the firewall security systems without needing to change the filtering rules.
- c. Ontologies, a formal representation of a set of concepts within a domain and the relationships between those concepts. Ontologies offer a direction towards solving the interoperability problems brought about by semantic obstacles, providing a common vocabulary for the area that defines with different levels, the meaning of the terms and the relationships between them.

4. Integrated legal and legislative information services. The experience of the library of congress of Chile.

Under the platform called LeyChile, the Library of the National Congress of Chile has adopted and applied the above-mentioned concepts to its management of information. It provides the Congress, in general, and the legislative process, in particular, integrated access to the legal documents that come from multiple legal sources within the country. Its main users are those who participate in the legislative process: primarily the members of Congress, the executive branch, the constitutional court, centres for the study of legislative matters, and those persons who operate and enforce legal regulations in the country. The Library, in its efforts to comply with the right to access public information, also provides services to citizens who request information or access to legal documents.

Conceptually these services are free and universal, certified since 2010 under ISO 9001:2008, and display an information management system based on interoperability, open data, XML standards, and offer Web services designed to share information with other systems and receive information from other applications with the concrete objective of facilitating user navigation and avoiding the duplication of processing tasks of legal documents in the various national institutions.

The most basic function of the Library of Congress is to provide information to be published in the official State publication (Diario Oficial) or in other authorized sources, in compliance with Chilean regulations. This system, however, forms just a part of an open and integrated platform of legal services based on the Web that allows the Library administer securely and accurately legal texts and other documents of interest, such as pending bills, legal history, constitutional, administrative or judicial rulings, and doctrine for the legislative process.

The integration of information can be of various types, from links, exchange of documents via web services, or access to previously published services from Library.

The Library carries out a process of analysis and value added to the documents that it stores to ensure their proper retrieval and, through the construction of an interoperable platform, allow for information to be exchanged with internal or external systems, independent of the technology used in those systems. The integration of the two systems depends on the technical feasibility that allows both systems to implement a standard mechanism of communication, with the exchange schema having been defined to such effect.

As mentioned, the services that transfer documents from the Library of Congress to users outside the Congress are free, use open standards, and are published in the public domain at the levels of data formatting, information exchange, and security. This means that their use, reuse, and redistribution to other users is authorized on a broad basis.

With respect to information security, the available platform conforms to high standards and the LNC is currently considering applying for certification under ISO 27001, which reflects the importance that the library affords its stored information.

5. Conclusions

The emergence of the network society constitutes a cultural, economic, and social revolution without precedent. It has impacted all members of society and all daily activities. With regard to the law, it is evident that it is affecting not only the traditional subject matter of legal doctrine, but also the entire prevailing legal culture itself.

Thus, the complex relationships between the law, technologies, and information are critical for the construction of a new legal culture under the rule of law, and that the right to information, information management, and information security are basic elements in meeting this challenge.

Contributions from these various disciplines have allowed for the development of modern legal documentation services based on interoperable open data, which, in turn, reflect the principles of free and universal access, the openness of data, and the emergence of global technologies and standards for exchanging and linking documents.

In Chile, the Library of Congress, through the LeyChile platform, is implementing a system of information management inspired by these principles.

It is likewise clear that the exigencies, latent in the rule of law, of affording access to legal documents will require further progress in implementing the principles considered here. Expanded access must be considered also to delivery to the public the law in ways that will facilitate the understanding of legislative matters and provide platforms that will enable users to contribute and interact in a Web 3.0 environment.

6. References

Decision 2004/387/EC of the European Parliament and of the Council of 21 April 2004 on the interoperable delivery of pan-European eGovernment services to public administrations, businesses and citizens (IDABC). Available in: [http://new.eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004D0387R\(01\)&rid=2](http://new.eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32004D0387R(01)&rid=2) [last visit: 30.04.2013]

Dijk, J.A.G.M. Van, De Netwerkmaatschappij, sociale aspecten van nieuwe media. Derde, herziene druk, Houten/Diegem, Bohn, Stafleu Van Loghum, 1997, 284 p.

García Arenas, María Isabel. Curso XML 1a. edición. Introducción. Disponible en http://www.bdw.freesevers.com/link_marlon/leng114.htm [last visit: 30.04.2013]

Legal Platform of Library of the National Congress of Chile (LeyChile). Available in: www.leychile.cl

Library of the National Congress of Chile. Available in www.bcn.cl

Principles of Open Government Data. Información en sitio web del grupo de trabajo. Available in: <http://www.opengovdata.org/home/8principles> [last visit: 30.04.2013]

Reyes, Patricia, Datos Gubernamentales Abiertos (Open Data Gov) en: Construyendo el e-G y la Sociedad del Conocimiento. Memorias de la VIII Conferencia Internacional de Derecho e Informática de La Habana. UNESCO (2011).

Reyes, Patricia, La Sociedad Red y el Gobierno de la Información. En Ciudadanas 2020. El gobierno de la Información. Editorial LOM, Santiago de Chile, pp. 193-205 (2011).

Reyes, Patricia, Gobierno Abierto. Una plataforma para un efectivo Derecho de Acceso a la Información Pública. En Ciudadanas 2020 II. El gobierno de la Información. Editorial LOM, Santiago de Chile, (2013).

Saarenpää, Ahti, Legal Informatics today, some theoretical observations. Santiago de Chile, (2011).

Saarenpää, Ahti, Legal well -being and Legal Informatics- the View from the University of Lapland. Finland (2012).

World Wide Web Consortium (W3C). Available in: <http://www.w3.org/>

FROM 'INFORMATION' TO 'NETWORK' SOCIETY: WHAT (IF ANYTHING) HAS CHANGED?

Marko Ampuja & Juha Koivisto

University of Helsinki, Finland,
Department of Social Research
marko.ampuja@helsinki.fi; juha.koivisto@uta.fi

Keywords: *Information society, Daniel Bell, Manuel Castells, innovation, state, neoliberalism*

Extended Abstract

Theories, discourses and policies associated with 'information society' emerged in the 1960s and have since become more prevalent in the academia as well as in policy planning in advanced industrial countries. Yet the discussions surrounding the topic have not remained constant over time; instead, major intellectual and conceptual shifts have occurred in information society theories and discourses in the previous four decades. Our presentation examined critically the conceptual-analytical shift from 'information society' to 'network society' by way of a close analysis of the work of Daniel Bell and Manuel Castells, arguably two of the most important information society thinkers. We maintain that this shift is not only related to technological developments but that it reflects a deeper political transition from Keynesian to neo-liberal policy regime. Most importantly, it has brought forward a different way of understanding the role of the state vis-à-vis the development of new information and communication technologies, as well as a new assessment of the role of the state in the economy and society at large.

In 1973, the year of the oil crisis, American sociologist Daniel Bell published his widely popular main work, *The Coming of the Post-Industrial Society*. The key argument by Bell was that industrial society was superseded by a different kind of 'postindustrial' society where human capital and the production of information and knowledge were responsible for economic growth, much more importantly than physical capital, energy creation and "muscle power". Bell argued that the post-industrial society would be increasingly technocratic, characterized by centralized state bureaucracies that managed large-scale systems of decision-making, science, innovation and economic production. Increasingly, Bell maintained, all advanced societies would become alike, governed not by the private-enterprise market system but by a strong post-industrial state. Thus, according to Bell, "the decisive social change taking place in our time ... is the subordination of the economic function to the political order", so that "the autonomy of the economic order (and the power of men who run it) is coming to an end" and "the control of society is no longer primarily economic but political".

In contrast to Bell, Manuel Castells, one of the most internationally acclaimed sociologists since the 1990s, has argued for an analysis of information society that disputes such overtly Keynesian conceptions of the state. In his *Information Age* -trilogy (originally published between 1996 and 1998) Castells argues that the power of the state is dissolving, especially due to new information and communication technologies that enable de-centralized political activities that resist state domination and hierarchical leadership. By the same token, Castells proposes that instead of centralized state bureaucracies, the capitalist markets are decisive for economic growth today, since

they have become more dynamic through the coming of “horizontal corporations” (such as Cisco Systems or Apple). These “network enterprises” are more flexible than before, capable of leading the way to a new, more innovative economy animated by “the spirit of informationalism”. The ‘network society’ thus signals the end of all kinds of ‘statist’ rigidities and hierarchies that are perceived as typical for industrial welfare states. Whereas Bell considered the state as the “political cockpit” that keeps information society in order, Castells thinks that the state needs to be kept in check, so that it would not interfere too much with the workings of the real engines of the information (or network) society, namely, visionary entrepreneurs, ‘hackers’ and risk capital investors.

Similar shifts towards neoliberal ideas concerning the state and the markets have become the staple of recent information society policies. In these policies the state is not seen to play a significant economic role by and itself, but its function is to guarantee favorable conditions for the operations of transnational capital. By contrast, the same policies consider markets as forces that are liberating consumers and citizens with the help of new information and communication technologies that are associated with fun, creativity and democratic emancipation – attributes that the industrial welfare state lacked, according to the same visions. Information society discourses have thus proven to be remarkably malleable, capable of being modified to comply with different political realities of different times. Yet the (still ongoing) global financial crisis that started in 2007–8 has posed many challenges and difficulties for the advocacy of information society theories and discourses today. The popularity of these discourses have hinged on their capacity to present ‘information society’ as a hopeful vision of progressive modernization. But due to the severity of the global financial crisis, the neoliberal information society vision has been undermined, at the same time as there are no strong signs of a return to Bell’s more Keynesian information society thinking (or policies). It remains to be seen if a new theory of information society will emerge that could rise up to meet the political and economic challenges that advanced capitalist countries face today.

[Our presentation in the KnowRight 2012 conference has been developed into a full-length referee-article manuscript that is currently under review with the title “From post-industrial to network society: The political conjunctures of information society theory”. Another related article, co-written by us, is “Strong and Weak Forms of Mediatization Theory: A Critical Review”, forthcoming in *Nordicom Review*.]

REGULATING THE NETWORK SOCIETY

A CHALLENGE FOR THE QUALITY OF LEGISLATION AND OTHER ACTIVITIES

Ahti Saarenpää

Professor of Private Law, Chair in Family Law, Law of Inheritance and Law of Personality
Director of the Institute for Law and Informatics, Faculty of Law, University of Lapland
Deputy Chair of the Data Protection Board, Finland.
asaarenp@ulapland.fi

Keywords: *Network society, legal welfare, information government, access, law-making, information law, dynamic documents*

Abstract: *The quality of legislation has long been the focus of debate in Europe. As such this is natural, even essential: in a democracy, legislation should be simple and clear. This is one of the fundamental elements of the constitutional state. Yet, as society has become more complex, the goal of simple and clear legislation has been steadily receding from reality. Risks from shortcomings in legislation and the failures of legislators have grown with the transition towards the new constitutional state in the Network Society. Our laws are nowadays deficient, hard to understand and hard to manage as a whole. In addition to the inherent difficulty of drafting and enacting laws, one key reason for the problems we encounter is the lack of a uniform doctrine of legislation. Legal theory has to accept much of the blame for this. The tools legislators have are inadequate. But then again we have also been slow to realise the new regulatory situations posed by the use of information technology and information networks. For example, this is one reason why the interoperability of information networks and information systems has long been neglected. Likewise, the central structural significance of personal data protection in the regulation in the Network Society is often forgotten. The rights of the individual easily yield to the needs of the market. This paper examines certain issues in the legal regulation of the new Network Society with particular reference to the general doctrines of legal welfare and Information Law. One of the main messages is, that regulating Network Society is not only regulating e-communication. It is much, much more.*

1. The quality of legislation

The quality of legislation has been a prominent topic in recent years, particularly in the European Union.¹ In Finland, as elsewhere, efforts have been put in place to monitor and improve the quality of drafting.² The issue is an important one if for no other reason than the fact that the quantity of

¹ EU Commission: “Better Regulation is a broad strategy to improve the regulatory environment in Europe - containing a range of initiatives to consolidate, codify and simplify existing legislation and improve the quality of new legislation by better evaluating its likely economic, social and environmental impacts.” See generally the Commission’s “Better Regulation” pages. See also the OECD’s “Guiding Principles for Regulatory Quality and Performance” and especially the OECD’s Better Regulation in Europe - The EU 15 project.

² See the web page on better regulation at oikeusministerio.fi/en/index/basicprovisions/legislation/parempisaantely.html

legislation is increasing steadily. Navigating the jungle of laws is more and more difficult. The traditional ideological aim that the average citizen should know the law and that ignorance of the law is no defence - *ignorantia iuris nocet* - is farther from reality than ever before. In Finland, the former Parliamentary Ombudsman, *Lauri Lehtimaja*, has aptly stated that in the EU today we - even lawyers - have to throw our hands up in surrender when it comes to the requirement of being familiar with legislation.³

Keeping the number of provisions in the law in check has long been one of the aims in steering regulation in Finland. In the 1990s we even spoke of "volunteer efforts" aimed at reducing the number.⁴ It was however a program to reduce norms. In the EU as well, quantitative goals have played a key role in programmes geared towards improved regulation. An illustrative example of how to approach this issue can be seen in the revision of the legislation on electronic communications that is currently underway in Finland. Efforts are being made to bring together key statutes into a single piece of legislation – the *Information Society Code*. The project is on-going but the present body of more than 450 provisions has already been reduced to 341. What is now a lot will decrease a lot - but will still be a lot.⁵

A second aim in drafting today has been to pay more attention to the views of different interest groups. This approach, known especially in the USA as *negotiated rule-making*, is unquestionably important if we are to avoid problems, mostly problems in practice with certain details. Indeed, drafting is often criticised for being too theoretical in nature. Negotiated rule-making is also a problematical procedure, however, as it often adheres too readily to the wishes of economic interest groups.

Copyright has been both a good and bad example in this regard. Some of the problems seen in the area of copyright today could have been avoided with a more broad-minded approach to the tension between the principle of the free flow of information and effective copyright. There has been a failure to anticipate the development of the *Network Society*, which is also an *access society*.⁶ Copyright today is one of the access rights too. The opportunities afforded by technology exceed the permissible boundaries, inadvertently creating a foundation for the rise of different extremist movements.

In broader terms, the crux of the issue is that it is difficult to find interest groups with the requisite expertise when it comes to many of the rights of the individual. For example, in Finland we as yet have no expert watchdog organisation even remotely on a par with *Privacy International* or *EPIC*, that is, one that would competently assess the development of the Network Society and individuals' rights in that society. To be sure, there are various civic organisations with varying degrees of expertise, but they are not to be considered as important or taken as seriously as a full-fledged watchdog organisation.

The number of provisions in our laws and proactive efforts to keep this number in check are not necessarily even the most important considerations when contemplating the legal regulation of the new Network Society. The development of the *Constitutional state* requires that there be more regulation than before. Individuals' rights – and, more importantly, any restrictions on those rights –

³ See *Lehtimaja Oikeutta eilen, tänään ja huomenna* (Law yesterday, today and tomorrow), LM 2010: 223 (in Finnish).

⁴ Between 1987-1991 the number of norms – acts, decrees and guidelines – decreased from 7600 to 5400. After that, the numbers have been higher, but the year 2012, which showed a decrease in the number of new government bills, was exceptional.

⁵ The draft bill has now been openly debated in Parliament since the beginning of April 2013.

⁶ The Network Society in my thinking is in a word a society in which we are dependent on information systems and information networks. Information systems and software applications are no longer merely tools which are acquired in response to the intermittent needs of the organizations or just for fun. We have a new important, challenging information infrastructure. My concept is quite near the more cultural concept of Network Society developed by *Jan van Dijk*. See *van Dijk Network Society* 3rd ed pp 22-48.

must be set out in the law. As I see things, this cannot be avoided – anywhere. It is not enough to think about different alternatives like information policies.⁷ Then again, in modern civil society expertise may not and cannot lie solely in legislative bodies. In a democracy, drafting must be broad in scope and open.

It is more important that we ask ourselves the question, do we have an acceptable, up-to-date doctrine of regulation? On balance, it seems the answer here would be negative.⁸ The doctrines we see in different countries focus more on technical considerations than on principles. Efforts to achieve clear legislation unify how individual Acts are enacted. At least this should be the case. But the principles vary on how provisions on different matters should be laid down. There is a lack of uniformity⁹. This is regrettable.

An illustrative example of this – one that will come as a surprise to many – is the regulation of personal data protection in Europe. The first Personal Data Acts in different countries were originally passed at different times. The Convention of the Council of Europe and the OECD Guidelines at the beginning of the 1980s harmonised the legislation that followed to some extent. However, it was only in 1995, with the adoption of the Personal Data Directive in the EU, that a more binding foundation was laid for regulation. Today, however, the legislative proposal for a new European General Personal Data Regulation, currently awaiting the approval of the European Parliament, is in part based on the view that the Directive did not achieve the desirable degree of harmonisation.¹⁰

In the field of law, it has occasionally been noted that harmonisation through European directives is in fact also a disharmonisation of sorts in that different countries look for ways to implement directives as they see fit in keeping with their legal cultures. This tendency has affected the data protection legislation on the protection of personal data. For example, in the Nordic countries, which have traditionally taken a quite uniform approach when it comes to private law, the legislation on personal data is formulated so differently from country to country that it is difficult to understand a neighbouring country's laws although they all comply with the same Personal Data Directive. A binding regulation could be the more effective tool to ensure uniform practice here.

We should of course also remember economic considerations when thinking about regulation. The jungle of laws is more and more expensive in daily use. That is why the new *Regulatory Fitness* programme published by the EU Commission in December 2012 may represent an improvement.¹¹ Administrative burdens are often expensive for users. However, regulatory fitness without deep-going critical analyses can in some situations be at odds with human and constitutional rights. We should not try to simplify too much.¹²

⁷ In recent years, the increase in information guidance has often been seen as a means to keep down the number of new pieces of legislation.

⁸ See also *Hoppe* Ex Ante evaluation of Legislation: between Puzzling and Powering pp 81-104 in *Verschuuren* (ed) *The Impact of Legislation*

⁹ I cannot go into detail on this in this paper and I will also have to content myself with merely mentioning the discussion about the different alternatives where regulation is concerned.

¹⁰ 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) 11 final.

¹¹ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: EU Regulatory Fitness {SWD(2012) 422 final} and {SWD(2012) 423 final}.

¹² *Wojciech Cyrul* has generally, without thinking about the deep structure of law, pointed out: "In lawmaking the intelligibility of the discourse is replaced by the explicitness of legal text. Although contemporarily legal texts are required to be both explicit and intelligible, paradoxically the more they are explicit the less they are intelligible." See *Cyrul* Lawmaking: Between Discourse and Legal Text. p 51 in *Wintgens* (ed) *Legislation in Context: Essays in Legisprudence*.

2. Human Rights and the Network Society

In addition to requiring technically unassailable legislation, the Constitutional state and the new Network Society pose challenges for the identification and development of substantive legal principles. Indeed, one must ask what are and should be the principles that must be safeguarded in legislation and when the legislator will possibly exceed the acceptable boundaries of those principles. Here we are operating on the level of both Human rights and Information Law.

An examination of this topic might best begin, perhaps somewhat surprisingly, with the impacts of the Convention on the *Right of Persons with Disabilities*, an instrument adopted by the UN in December 2006 and already ratified by a large number of countries.¹³ The Convention states that people are to be as equal as possible regardless of personal disabilities. An essential corollary to this is the idea of an inclusive, borderless network society. This principle was approved by the EU in the 2006 e-Government Action Plan (COM 2006 173)¹⁴. Everyone is to have *access to networks*; no one may be left behind. This can and should be construed as a fundamental and human right¹⁵. We live in what, in a word, may be called the “Age of Access” in the Network Society. The impacts of the Digital Divide that we spoke about so much at one time should be constantly more and more minimised.

In a broader sense, access to networks should also be financially within the reach of as many people as possible. Here we encounter a clear shortcoming in the substantive doctrine of legislation. Regulating *infrastructures* has a long tradition on the technical level, one good example being the guaranteed compatibility of telecommunications networks. In other respects, however, we lack general principles on how to regulate infrastructures and their use. There was no real need for such principles when it was natural that the state had ultimate responsibility for how infrastructures worked. However, the liberalisation of telecommunications in Europe in the 1990s resulted in a situation where the markets for electronic communications were regulated without much in the way of agreed principles. This shortcoming was no doubt the reason why we saw auctions of operator licenses and frequencies.

Partially as a result of this development, electronic communications became quite expensive indeed, and instead of providing basic services the major operators began looking for international investment opportunities. When the *General Services Directive* was adopted in 2002, it represented a certain change of direction towards a better *right to communication* for individuals. Yet, in Finland, for example, as we enter the new 4G age, we are again auctioning frequencies. The goal is to bring in at least 100 million euros in revenue for the state.¹⁶ But genuine infrastructures should be inexpensive for citizens. In the Network Society this is a particularly salient point and need, since almost all of us are dependent on networks. Auctioning does give wrong signals.

3. Interoperability

One problem in its own right is the lack of *interoperability*, which has long plagued computer software and information systems. The EU took a position on the issue in copyright legislation back in the early 1990s when it allowed reverse engineering. Article 6 of the 1991 EU Computer Programs

¹³ In May 2013 totally 130 states had ratified the Convention.

¹⁴ COM(2006) 173 final : i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All.

¹⁵ In his report to the UN Council of Human Rights in 2011, Special Rapporteur *Frank La Rue* put forward the view that access should be understood as a human right. See UN General Assembly A/HRC/17/27. I would add to this discussion the question of Internet neutrality too. In this paper I consciously do not discuss about the governance of Internet.

¹⁶ Auctions in Finland are based on the 2009 Act on auctioning certain radio frequencies. The original idea of auction was published by professor *Ronald Coase* in 1959 – in an age long time before our modern Constitutional State and Network Society.

Directive allows reverse engineering for the purposes of interoperability. This was a crucial step forwards for society at large, although unfortunately it has often been seen only as a technological development.

In the Network Society, the matter has come to the fore in a new way. Problems with *interoperability* must not disrupt the smooth functioning of government. Accordingly Finland enacted – but not until 2011 – the *Act on Information Management Governance in Public Administration*, whose particular objective is to promote interoperability. Section 1 states: “The purpose of this Act is to improve the efficiency of activities in public administration and to improve public services and their availability by laying down provisions on information management in public administration and on promoting and ensuring the interoperability of information systems.”

The background to the law is straightforward: the extensive incompatibility of software applications and the use of data systems in the public sector. This has been particularly visible and harmful in social welfare and public health care. In that sector, the independence of Finnish municipalities had resulted in there being a wide variety of information systems and software acquisitions. In the early days of the application of the law, a similar situation occurred with the idiosyncratic nature of the application LotusNotes, which was introduced in the courts of appeal. The software prevented reliable and straightforward contact with other courts and with clients. And problems occurred even when trying to share documents within the same court.

One interesting point is that Finnish universities opposed the law when it was being drafted, appealing to their independence and need for special software. Some of the opposition seems to have been based on a failure to distinguish between electronic communications as a fundamental necessity in the Network Society and the needs of universities in the areas of research and teaching. The universities cannot remain outside of the electronic communications infrastructure in the Network Society.

Today, the new Act provides a framework for building a new comprehensive architecture for information management in government. The issue thus goes beyond merely concentrating purchases of software. The aims are compatibility, comprehensive architecture, information security and, in the final analysis, cost savings as well.¹⁷ Thinking of and purchasing information systems and software applications as separate tools has cost the country millions of euros in money and working time.

This is not merely a national question however. The EU as a whole is an area where interoperability in public administration is more and more important. From the older interoperability of railways we are now taking steps towards European interoperability in public administration. The European Commission already has a special programme in place for the purpose, ISA.¹⁸ From the legal point of view it is extremely challenging.¹⁹

4. Information security

Another matter that has long been overlooked in legislation is *information security*. We find ourselves in a special situation where the protection of personal data is a fundamental right but information security – absolutely essential for effective data protection – is not. There have no doubt

¹⁷ See generally Using services and information: A proposal for the first common strategy to address challenges in public sector ICT utilisation 2012 – 2020, Finnish Ministry of Finance.

¹⁸ See more at ec.europa.eu/isa/index_en.htm. and COM(2010) 744 Towards interoperability for European public services

¹⁹ The following words written by *Franziska Boehm* are alarming even in this programme: “The rights of individuals as regards their interest in knowing in which of the existing EU databases their personal data are processed seems to be subordinated to security interest. The missing notification duty about transfers having taken place is one of the shortcomings. If introduced, it would considerably improve the knowledge of the whereabouts of personal data.” See *Boehm* Information Sharing and Data Protection in the Area of Freedom, Security and Justice p. 426

been political reasons for this in Europe. Regulations on information security are closely associated with security in broader terms, making it hard from the very beginning to legislate matters through a security directive. One must bear in mind that the European Personal Data Directive did not originally apply to public order and security. It is also telling that when it was established, the European Network and Information Security Agency (ENISA) was – and after some amendments to the related regulation still is – temporary in nature.²⁰

In Finland, information security has been comprehensive from the very outset, covering the work of the Finnish Police, Border Guard and the Defence Forces alike. The special provisions on personal data protection in these sectors have been laid down in special laws. Information security is of course included in the 1995 Personal Data Directive but receives rather scanty attention in the instrument. The implementation of information security was subject to the principle of *proportionality*: it had to be adequate in relation to the nature of the information and the costs involved. This is in fact natural. We should not create too many expensive administrative burdens because of information security. Yet, this wide open approach to regulation resulted in weak, somewhat “sparing” information security. Maximal and minimal levels can be surprisingly near each other when thinking about information security.

I should also point out that in the 1990s we were slow in Europe to realise the importance of information security. It fell between the cracks, so to speak, in the research and teaching in IT. And given that the *European Charter of Fundamental Rights* was drafted back in the 1990s, it is no wonder that the importance of information security was not given adequate attention in the instrument. The Charter is quite timely in many respects but where the relation between data protection and information security is concerned, it reflects an era that is now already very much past.

After the 1990s, we see information security being taken more seriously. The increased computerisation of traditional crimes, extensive cases of hacking, and denial-of-service attacks have all served as wake-up calls. Nevertheless, a new report of the Finnish Data Protection Ombudsman indicates that one-third of companies that had problems with information security did nothing after the fact to improve matters.²¹ And one of the cardinal sins in using information networks – using unprotected email – is still common practice. Even attorneys in Finland are guilty of this in correspondence with their clients and courts.²² The present insecure state of the infrastructure is not duly acknowledged and there is a fear that strong user authentication will scare customers away.

In terms of regulation, information security is both hard and easy. It would be easy to promote it to being a fundamental right. Everyone should have access to secure information networks, a right to secure connections when communicating with government authorities, different organisations and the markets. This is one of the central principles of the general doctrines of modern *Information Law*.²³ The path that the average citizen's information travels and the distribution of digital products among various computer terminals must be made secure. This is an inseparable element of *legal welfare* in the Network Society. One of the core principles here is to avoid legal problems from the outset if possible. Today our rights should be realised as early as possible in any process.²⁴

It is harder to regulate the standard of information security on a level more detailed than the principle of proportionality. Information security is of course one of those issues which requires technol-

²⁰ Regulation 580/2011 of the European Parliament and of the Council of 8th June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

²¹ www.tietosuoja.fi/59848.htm (in Finnish).

²² In Finland, the Parliamentary Ombudsman has, and with good reason, taken the clear position that confidential information may not be sent using an unprotected email account.

²³ See for example *Saarenpää* The Importance of Information Security in Safeguarding Human and Fundamental Rights in *Greenstein* Vem reglerar Informationsamhället? (2010) p. 45.

²⁴ See more *Saarenpää* Legal welfare and legal planning in the network society pp 47-69 in *Barzallo – Valdés – Reyes – Amoroso* (eds) XVI Congreso Iberoamericano de Derecho e Informática (2012).

ogy-neutral legislation. Nevertheless, we can identify at least two instances in which a better approach has been found. One can be seen in the successful provisions on strong authentication of individuals in directives at the EU level. Another is the step taken in the form of legislation on personal data protection towards acknowledging the increased importance of standards and certifications.²⁵

In addition, I would hasten to point out that the status of personal data protection as an express European fundamental right should in itself affect the interpretation of what the standard of information security should be. Data protection authorities, whose competence and resources are being increased as part of the reform of data protection legislation in Europe, in future have better legal means at their disposal. This is something very important in the practical use of technical information security tools and should have a world-wide effect.

One element that can be used to signal the importance of information security is monitoring of vulnerabilities. The new European Data Protection Regulation will contain an express obligation for those processing personal data to report on any data breach problems that emerge. A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed must be reported. The traditional approach of keeping data breach problems inside organisations is no longer acceptable.²⁶

This is in fact a natural, essential approach to the matter. A somewhat harder nut to crack is how the search for vulnerabilities should be organised. CERTs (Computer Emergency Response Teams) were originally based on scientific interest and their work was carried out on a volunteer basis. In many countries, Finland included, this work has since developed to become a government activity. And to a large extent it is also a question of a commercial opportunity for information security companies.

To date, everything has been based on the fact that it has been easy to monitor activities on networks. Information networks are, in a sense, new public forums. In the final analysis, however, one must ask whether, for example, the established practice of the copyright organisations – monitoring communications on networks using IT agents with no provisions in the law to back them up – really conforms to the principles of confidential communication in the developing constitutional state. Here we can see the old spectre of the surveillance society joined by a newer threat that one might term “surveillance markets”. And in any case the work of CERTs must be regulated by law even when it is being carried out by parties other than government officials.²⁷

The practical standard of information security can also be improved indirectly through the appointment of data protection officers. The management of a company or public office, mindful of security, appoints a data protection officer to guide and monitor the standard of data protection and, at the same time, information security in the organisation. In the Nordic countries, Sweden has been a pioneer in this respect. In Finland social welfare and healthcare units will soon have data protection officers. And the new European Personal Data Regulation will make it mandatory to appoint a data protection officer in all public authorities as well as in private companies employing more than 250 people.²⁸ Clearly, at its best, an organisation's ordinary internal monitoring can reveal data protec-

²⁵ See especially Data Protection Standard SFS-ISO/IEC 29100:2011 and the EU Draft Regulation article 23.

²⁶ See the Draft Regulation articles 31 and 32.

²⁷ In Finland, CERT is part of the Finnish Communications Regulatory Authority and its work is regulated by the Act on the Protection of Privacy in Electronic Communications. The regulation is quite vague, however, which shows that when the Act was enacted in 2004 no one realised the societal significance of CERT's work and its need to be independent.

²⁸ As the number of personnel is not necessarily an accurate indicator of the amount of information involved. That is why the rapporteur of the European Parliament, *Jean-Philipp Albrecht*, has proposed in his report – 2012/0011(COD) – that the amount of information should be taken into account in determining when a data protection officer must be engaged. Mr *Albrecht* has passed the EULISP LLM program in legal informatics.

tion and information security problems, but with data protection officers management is improved in that it takes into account more sophisticated information security and personal data protection. One of the key concepts in modern personal data protection – *accountability* – plays a prominent role here.

Thus, information security is the second principal starting-point, after human rights, in the legal regulation of the Network Society. Every time we access a network our legal status is at risk: there is someone out there trying to invade our personal data and privacy, gathering information on us and monitoring our communications.

To cite one example, in e-Commerce the prices of different travel tickets and packages may vary depending on how the company selling them has profiled us. Although the problems associated with such profiling have been discussed for a long time, in terms of individuals' rights the situation has not really improved. Interestingly, the new report of the Finnish Data Protection Ombudsman notes that many businesses were unable to demonstrate what benefits profiling brings them in real terms. They profile but they do not know exactly why. And some of the companies do not tell customers that they are profiling.²⁹

What is more, in the new information government, authorities collect more and more information on us. The old spectre of the “Naked Society” is still with us, although the European Personal Data Directive, adopted back in the 1990s, sought to diminish it. The threat was simply not taken seriously enough.

Today, we see *transparency* – a hot topic throughout the world – giving rise to new tensions. It seems difficult to reconcile sound transparency with good personal data protection. Yet, transparency is something which should work primarily for citizens, not against them. When we work in the new Information Government with the outdated information systems of the old eGovernment, it is hard to avoid problems – even if human rights are duly respected. Administrative burdens make easy solutions attractive. For example, implementing the basically sound principle of open data causes difficulties where personal data protection is concerned.³⁰ Most registers and archives are personal data registers.

The regulation of personal data protection brought in the concept of *informed consent*, which had been used particularly in the context of health law. The idea in itself is a sound one. As a rule, our personal data may only be used for purposes we ourselves approve of. In practice, however, this has caused any number of problems as data controllers have tried to implement consent that is as open as possible. Where people do not understand the meaning of the term, it is easy to secure all kinds of consent. One way to rectify this situation would be to enact a comprehensive special law on the phenomenon of informed consent and create law-specific digital approvals with a sufficient information base. The typical approach today, where we simply acknowledge receipt of information provided in any variety of ways, would no longer be adequate.³¹

5. Information law

Information Law is a field where teaching and research focus on issues connected with information and digital communication. It is part of the field of Legal Informatics at the University of Lapland and more generally. Legal Informatics, which concerns itself with modern IT, is over half a century old as a science – as old as the computer. In contrast, Information Law has quite a shorter history. The bases of Information Law were probably first discussed in Germany in the 1970s and in the

²⁹ Data Protection Ombudsman 27.01.2012 (in Finnish).

³⁰ Cfr Janssen, Katleen The PSI directive – running behind before it even started pp 129-139 in *Schweighofer – Gaster – Farrand* KnowRight 2010.

³¹ Cfr EU Draft regulation recital 25.

Nordic countries and Belgium in the 1980s. For a long time, however, doubts were voiced to the effect that it was impossible to find common principles that would encompass copyright, telecommunications, data protection and the principle of openness.

There is no place for such doubts today – or at least there should not be. Five basic reasons tell us why: (1) the heightened significance of fundamental rights, (2) digital convergence, (3) digital information processes as the environment in which we as a society work, (4) the transition from eGovernment to information government, and (5) the transition from the Information Society to the Network Society. I have already discussed these considerations but they merit a look in terms of the categories we rely on in classifying law. The focus here is detecting a need to change how we classify law, as this classification reflects what is important at any given time. Overall, the importance of information in society has changed. It is no longer merely the raw material for more important matters and procedures. We are living in a world of information processes.³²

The heightened importance of human and fundamental rights does not allow for laws that are geared to the aims of different interest groups and at the same time restrict the rights of the individual; nor is there room for what are known as best practices, whose purpose is essentially the same. The point of departure in everything is the individual's right to self-determination and respect for human dignity.³³ Digital convergence, a phenomenon noticed already in the 1990s if not before, brought what was largely specialised regulation and drafting under the same umbrella of principles. The same tools are now the means for exercising a wide range of rights. The legal conflicts between these must be detected in good time. Our *right to know* based on the self-determination is and must always be the leading principle of Information Law.

Likewise, it is time to say good-bye to eGovernment. This was government in which IT produced tools for government. In today's information government we are dependent on a digital operating environment and the average citizen's electronic link to government is more interactive and takes place more in real time than before. The new *Citizen's Account* service in Finland is a good example of this development. It allows individuals to follow the progress of their affairs in government on information networks with a protected connection.³⁴ This is a concrete implementation of modern transparency in today's digital environment.

And, lastly, once again we must remember the transition to the Network Society. In addition to considerations of fundamental rights, the new Network Society highlights the equality of citizens more than before. The slogan of the European Commission says it all: "No one will be left behind." We have made considerable progress from the days when computers were primarily tools for enthusiasts and for back office operations in government. The long-standing division between front- and back-office thinking is over.

All of these changes have made Information Law a more important area than ever within Legal Informatics and they are being given an increasingly prominent role in the discipline. A good lawyer simply cannot survive without a sound knowledge of Information Law. He or she must know the main principles in the field of Information Law to be able to handle the jungle of legislation. Those principles are the right to know, the right to information, the right to communication, freedom of information, the free flow of information, the right to informational self-determination and the right to information security. These principles help us to better understand the world of information processes. In legal terms, what we have is much more than a collection of separate acts and decrees with different purposes.

³² See more *Saarenpää Perspectives on Privacy* pp. 58 in *Saarenpää* (ed) *Legal Privacy*.

³³ Cfr. *Kateb, George Human Dignity*, passim.

³⁴ See basic information at asiointitili.suomi.fi/.

We need to see a solid investment of resources in basic teaching and professional development in the field as part of the legal education. And in terms of legal design (planning) we need to see more training that is geared to legal quality and that seeks to develop a common understanding among the relevant professions. One thing that should not be allowed – to cite just one example – is entrepreneurship that is being taught without taking into account the fundamental importance of personal data protection in all business activities. Unfortunately, examples of this can be found even in Finland.³⁵

6. Some examples

Thus far, I have largely discussed the issues on the level of the principles involved. They are the core of all legal thinking. In closing, I would like to present some examples dealing more with actual practice. They all relate at least partly to personal data protection. The reason for this choice is clear. Data protection is nowadays a European fundamental right whose scope is very broad indeed, so much so that it even surprises those with a solid understanding of the field. In the world of information processes it is difficult to find situations where data protection is not somehow involved. For this reason, I call it an “everyday fundamental right”.

We need go no further than email to see the nature of personal data protection as an everyday fundamental right. We often use it without particular concern. We do not protect our mail and we use email systems which monitor the content of the messages. What is even more peculiar is that in most Finnish universities the password for email is the same as that used in other applications. This is unequivocally contrary to the law. Use of the same password for several purposes compromises two fundamental rights: the protection of personal data and the protection of confidential communication. Not even the proportionality in the information security provision of the Finnish Personal Data Act gives any leeway to accept such a procedure. A good lawyer would notice immediately that the practice of the Finnish universities is flawed here. It is a matter of fact, not only interpretation.

My second example is general in nature. We have now entered the world of digital estates. When a person dies, the question arises of what to do with his or her email.

This is a general question and where the public sector is concerned a special one. It is a general concern that in Finland, unlike certain other countries, the protection of personal data continues even after a person dies. It is a special question in that email in the public sector in most countries became somewhat of a hybrid due to shortcomings in legal planning, meaning that it allowed both work-related and private mail. In Finland, this problem was later solved in favour of the employee through the Act on Privacy in the Workplace. An employer has essentially no legal opportunity to access an email received or sent by an employee. Nor does the even internationally well-known *Lex Nokia* allow this. If that law were actually used, it would only make it possible to detect exceptional email traffic in special situations. However there are no companies using that Act nowadays in Finland.³⁶

What then can be done after a person has died? Many organisations have begun to turn over a deceased person's *emails* to his or her heirs. The rationale here is that everything is inherited. And

³⁵ Even my own university has given entrepreneurship training in recent years where the legal studies have focused on contracts and taxation with personal data protection and other aspects of Information Law dropped from the programme. The change of Society has not been taken into account when planning teaching program.

³⁶ The law known as *Lex Nokia*, which provides for a limited right for organisations maintaining their own internal information networks to monitor exceptional email activity among employees and other members of the organisation, requires an information security plan approved by the Data Protection Ombudsman. To date – April 2013 – only one organisation, a town has submitted a notification to the Ombudsman indicating that it plans to begin such monitoring, and this is intended to monitor for malware. This provision will not be found in the future Information Society Code.

because the legislation governing inheritance in most countries has no special provisions on email, heirs acquire control over email messages. This approach can be considered conservative, even ultraconservative. It also reflects a scanty knowledge of the general principles of the law of personality.³⁷

The more appropriate approach, given the lack of express regulation, would be to assess what the effect of human and fundamental rights is where personal data protection continues as a fundamental right after death. For example, in the case of data on our health the matter has been resolved in Finland in the Patient Rights Act. The medical records of a deceased person are not as such passed to his or her heirs, but even persons other than the heirs may obtain the information if this is essential for the exercise of the potential recipient's rights. Thus, personal data protection in Finland extends to the time after a person's death. This was the premise adopted when the country's very first Personal Data Protection Act was drafted and applied. Although the Personal Data Directive has no provisions on the information of deceased persons, domestic legislation may be applied in such cases. Indeed, when enacting the Personal Data Act, which implemented the Directive in Finland, there was never even any suggestion that its provisions would be limited in application to living persons only. There was no desire to restrict personal data protection.

In principle, emails should not be handed over to the heirs unless the testator has made a specific request to this effect. Unfortunately, as yet there are no provisions governing this matter in the Code of Inheritance or the Act on Personal Data Protection in Electronic Communication. In other particulars as well, the Finnish Code of Inheritance requires a reassessment where matters of privacy, data protection and law of personality generally are concerned. And I dare say Finland is not alone in this regard.³⁸

My third example involves personal credit information. This is a crucial issue where an individual's identity is concerned. The question is when, how and to what extent others have a right to obtain information about our financial status. Debtor identity can be harmful in many situations.

Different countries have adopted different solutions here. Credit data registers are maintained by the government or the private sector either freely or with guidance. The registers are either positive, meaning they have extensive information on a person's financial standing, or negative, meaning that they contain data on credit defaults only. However, a clear majority of EU member states, for example, has traditionally permitted the use of positive credit data registers. This legislative tradition has its roots from the age before data protection legislation.

Thus far, in Finland we have confined ourselves to keeping commercial negative credit data registers only. Recent years have seen increasing demands for a transition to using positive credit data as well. In fact the Government Programme notes that the issue should be examined. Accordingly, the Ministry of Justice commissioned me to draw up a detailed assessment, which I completed in April 2013. My assessment concluded with a proposal that for the time being we should continue to use the present system based negative credit data. The principal reasons for this position were the increasing self-determination – including economic self-determination – of the individual in the European constitutional state, the significance of the economic identity of the individual in society, the on-going reform of data protection legislation in Europe and the question of what kind of central

³⁷ About the law of personality see for example *Saarenpää Perspectives on Privacy* pp 47-57 in *Saarenpää* (ed) *Legal Privacy*.

³⁸ Unfortunately the *Finnish Communications Regulatory Authority* has recently taken the position that an operator may hand over the information of a dead person to his or her heirs. This view is clearly erroneous in terms of data protection legislation. The legislation should be amended without delay to preclude such misleading interpretations. It should be more informative for non-professionals too.

register the change to using positive credit data would require and who would be in charge of maintaining that register.³⁹

The issue of regulating the collection and use of credit data highlights a component of quality that is crucial but often forgotten – particularly when comparing regulation in different countries. The heightened importance of human and fundamental rights in the modern constitutional state always requires a careful test to ensure the safeguarding of those rights when changing an old system and planning a new one. In the Network Society this test cannot yield to technological, economic or general societal considerations. What has evolved in the days before the present constitutional state will no longer necessarily suffice as a model for new legislation in that state and in the Network Society.

My fourth example brings us into the realm of *document logistics* or document workflow. This is an area that has been sadly alien to lawyers in the field. Lawyers are experts when it comes to documents but not when it comes to document logistics.

I personally use “document logistics” today as a theoretical basic concept, which opens up a perspective on the life-cycle of different documents. In today’s information government, document logistics plays a crucial role in both law and government. Sound logistics serves to ensure that on any given occasion the correct information is in the right form, provided in the right manner, at the right time and placed in the hands of the right party. In other words, every effort should be made to optimise the path information travels, which is one of the central aims of the constitutional state. This requires well-developed *legal planning* – legal design – of documents and information systems alike. And it is of course connected to the idea of interoperability too.

It is essential to point out that document logistics involves more than just the content of documents. The fundamental questions begin with how different types of data are attached: what computer platform is being used, in what computer environment, by whom, and with what technology – especially the mark-up language. And the list does not end here. We also have to ask how the information security of the documents will be ensured; to whom, how and in what form the data will be delivered; and what the life-cycle of the data will be.

These questions are not always asked, putting it mildly. There are lawyers and other legal actors who draft documents as they see fit, as static messages to others. The path that information takes is not considered at all. An illustrative, albeit regrettable, example of a technically outdated procedure and the dubious approval it enjoys under the law can be found in a very recent decision of the Finnish Supreme Administrative Court (KHO:2013:28). In the case, the highest guidance body in the patient rights system, the Patient Injuries Board, refused to provide decisions made in its plenary sessions to a law firm that had requested them. The Board is a governmental body and as such is subject to the principle of openness. Nevertheless, the decisions were not given to the law office. One reason was that the decisions had been written in a manner that made them hard to understand with the personal data crossed out. As document logistics had been overlooked, the Supreme Administrative Court’s interpretation violated the applicable principle of openness in Finland. This should not have been possible. But this is what happened.⁴⁰ We could say about many lawyers and

³⁹ My report has been published in Finnish on the web pages of the Ministry of Justice at oikeusministerio.fi/fi/index/julkaisut/julkaisuarkisto/1366713053579.html. See also on the basic issues related to the topic *Saarenpää* The Debtor Identity: Perspectives on Collecting Credit Information and Regulating its Use pp 457-468 in *Schweighofer, Erich – Kummer, Franz – Hötzendorfer, Walter* (Eds.), *Abstraktion und Applikation Tagungsband des 16. Internationalen Rechtinformatik Symposions IRIS 2013 Proceeding of the 16th International Legal Informatics Symposium*.

⁴⁰ The lower court had reached a different conclusion. It would have ordered the decisions to be released with the amount of text overstruck that was necessary to prevent personal data from being disclosed. One member of the Supreme Administrative Court was of the same opinion.

legislators in this situation the following: they are practical users of IT but practically useless with the role of IT.

7. Conclusions

After what I have said about the foregoing topics, it is appropriate to go back briefly to the central points of departure in this paper. We are living in an era of remarkable changes. We are entering an era whose distinctive developments are the Network Society and the new constitutional state. In the Network Society we are dependent on the smooth functioning of information systems; in the new constitutional state we rely on legal welfare, which is based on human rights. In these contexts, the individual's right of self-determination takes on heightened importance and the expectation is that his or her rights will be acknowledged and accommodated earlier on in all information processes – not only legal processes.⁴¹

These changes suggest that we should round out our views on the doctrine of legislation. It is not enough for us to try to produce clear and practically oriented laws in which procedure and sanctions play the central role. We must also take a closer look at the information processes and document logistics relating to different issues and phenomena. This was not necessary when computers were mere tools helping us in what we did. Today the situation has changed markedly. We must take into consideration the path that data must travel as a whole. Even the choice of computer environment is crucial from the perspective of fundamental rights and a factor that has to be considered when drafting legislation.

In addition to this general change in attitude, it is important, even essential, that we create a new conception of what a *document* is. We need to introduce the concept of a dynamic document; to date documents have mostly been static. The new concept must be adopted and applied in legislation and in order to properly safeguard personal data protection, privacy, confidentiality and the media's need for information. The days when documents had sections overstruck at the controller's discretion when they were released to recipients should be well behind us.⁴²

I have written rather much about personal data protection in this paper, which may seem puzzling. There is of course more to the Network Society, much more, than the processing of personal data. I am well aware of this, as should be apparent from what I have presented here. One reason for selecting examples relating to personal data protection is that they are closely related to legal practice. However, there is a second, complementary reason that makes a focus on legislation in that field worthwhile: it constitutes one of the first significant bodies of law in the Network Society.

We have seen much progress from the days of the Swedish Datalag, which more than anything reflected uncertainty about the impacts of IT, to the regulation of the life-cycle of information processes on networks and beyond them as well. The soon-to-be-adopted EU Personal Data Regulation, which retains the principles we have adopted, will strengthen the structural whole of regulation. The emphasis on accountability, data protection by design and data protection by default as key concepts highlights the significance of managing information processes more than it has been

⁴¹ Those observations have also been pivotal starting points in our international and interdisciplinary research project NETSO: Network Society as a Paradigm for Legal and Societal Thinking. Project is funded by the Academy of Finland.

⁴² The Finnish Personal Data Act has adopted the notion of a *dynamic document* to a limited extent. Section 13.4 states: „The controller shall see to that the personal identity number is not unnecessarily included in hard copies printed or drawn up from the personal data file.”

heretofore.⁴³ At the same time this regulation as such functions as a good structural example of technology-neutral regulation in the Network Society.

Likewise it is important to remember that the comparatively – but not wholly - new idea of *open data* is closely connected to other aspects of Information Law. The recycling of information gathered by the public sector is part of the new openness and transparency of society. Information should be freely available, not only for sale.⁴⁴ This is a clear societal principle that has recently been embraced in both Europe and the United States.⁴⁵ Efforts to implement the principle will run into significant barriers in the area of Information Law. A very large number of documents contain personal data or information protected by copyright. This means that the implementation of open data will be very limited unless a massive conversion of data is undertaken and unless dynamic documents are used when new information is produced.⁴⁶

In concluding, I would like to say that as far back as – or perhaps not until – 1997 the Institute for Law and Informatics at the University of Lapland proposed in a report that a new general Information Security Act should be enacted in Finland.⁴⁷ Among other things, we noticed that personal data protection and information security should be in balance. They were not. Likewise, we observed that cyber security had to be taken seriously. Although the Parliamentary Ombudsman, for example, spoke in favour of starting work on the law, our proposal did not lead to any immediate results. Perceptions of the need for new legislation differed considerably. The new significance of IT was still unfamiliar to many or was at least a somewhat dubious affair.

Today we can say in Finland that we have made some progress in this area of regulation. Information security in the public sector is guided by the Information Security Decree, enacted in 2009, and specific regulations exist governing the assessment of data security in public authorities.⁴⁸ Yet, I am still of the opinion that a general law on information security should be an important part of the foundation of a constitutional state. Today the law that we first proposed would be very different however, with more of an emphasis on human and fundamental rights. Information security may very well have become the most challenging legislative concern we face today. An insecure information infrastructure has no place in the constitutional state of the Network Society. For this reason, it is a welcome sign that the EU is finally waking up to more general regulation in the area of information security.⁴⁹ We are more and more using our fundamental rights in the e-communication environment. Having no more than criminal sanctions against cybercrimes has for a long time already been a burying of our heads in the sand.

In the digital environment we should also think about the need to make legislation easier to understand through a new kind of legislation: *interactive legislation*. The age of using traditional linear text only should be over.

⁴³ I should mention that all three of these matters are in principle regulated in the present Finnish Personal Data Act although these particular terms are not used.

⁴⁴ See generally COM(2011) 882 final Open data: An engine for innovation, growth and transparent governance

⁴⁵ See www.whitehouse.gov/open

⁴⁶ Cfr Balthasar, Alexander – Prosser, Alexander Open data = All Public Data free? Fragen anhand der bevorstehenden Änderung der PSI-Richtlinie pp. 295-302 in Schweighofer – Kummer – Hötzendorfer (Eds.), Abstraktion und Applikation Tagungsband des 16. Internationalen Rechtinformatik Symposions IRIS 2013 Proceeding of the 16th International Legal Informatics Symposium.

⁴⁷ Saarenpää-Pöysti (ed) Tietoturvallisuus ja laki: näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä (in Finnish).

⁴⁸ It is odd here that the Information Security Decree is only a decree, a lower-level norm than an Act. Yet the provisions on the assessment of information security are set out in an Act. The use of a decree reflects the old-fashioned thinking whereby information security is considered no more than a tool.

⁴⁹ See especially Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - COM(2013) 48 final - 7/2/2013 - EN

By interactive legislation I mean legislation in which the text of the laws is accompanied by information on its background and its broader context. In other words, some of the information found typically in the legal literature today would be presented in conjunction with legislation as text references that would appear in the electronic collection of statutes. The user of the text could obtain additional information on the relevant points as they are made actively available in the information space.

This change would require that we adopt a new concept of legislation in the Network Society. On the technical level, the new form of legislation would be easy to implement. It would be presented into a more readily comprehensible form in terms of its depth of source, which would serve layperson and lawyer alike. Unfortunately opportunities such as these have gone virtually unnoticed in efforts to improve legislation.⁵⁰ It is time to understand better regulation as a whole extending from the digital template to a form displaying the deep structure of the law. This would at the same time be part of a new and essential justice respecting informational rights on the societal level.⁵¹ Let me at the end of the day once again repeat my starting point: in a democracy, legislation should be simple and clear.⁵² This is one of the fundamental elements of the constitutional state in the Network Society. That is why we do need a new concept of legislation. The age of separated linear texts as legislation should be over.

8. References

- Balthasar, Alexander – Prosser, Alexander* Open Data = All Public Data free? Fragen anhand der bevorstehenden Änderung der PSI-Richtlinie pp. 295-302 in Schweighofer – Kummer – Hötzendorfer (Eds.), Abstraktion und Applikation Tagungsband des 16. Internationalen Recht-informatik Symposions IRIS 2013 Proceeding of the 16th International Legal Informatics Symposium.
- Boehm Franziska* Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Springer 2012
- van Dijk, Jan* Network Society 3rd ed. Sage publications (2012)
- Greenstein, Stanley* Vem reglerar Informationssamhället? pp. 45. Jure (2010).
- Hoeren, Thomas* Eine kontraktualistische Konzeption der Informationsgerechtigkeit - A contractualist conception of information justice, Rechtstheorie 2003 p. 333
- Hoeren, Thomas* Informationsgerechtigkeit als Leitperspektive des Informationsrechts pp 91-102 in *Taege-Wiebe* (Hrsg) Informatik-Wirtschaft-Recht. Regulierung in der Wissensgesellschaft.
- Hoppe, Robert* Ex Ante evaluation of Legislation: between Puzzling and Powering pp 81-104 in Verschuuren (ed) The Impact of Legislation.
- Janssen, Katleen* The PSI directive – running behind before it even started pp 129-139 in *Schweighofer – Gaster – Farrand* KnowRight 2010
- Kateb, George* Human Dignity, Belknap Press (2011)

⁵⁰ See also *Saarenpää* The Network Society and legal information. Some observations from the Nordic point of view. in www.hklii.hk/conference/paper/2D1.pdf

⁵¹ On this principle see *Hoeren* Eine kontraktualistische Konzeption der Informationsgerechtigkeit - A contractualist conception of information justice, Rechtstheorie 2003 p. 333 and especially *Hoeren* Informationsgerechtigkeit als Leitperspektive des Informationsrechts pp 91-102 in *Taege-Wiebe* (Hrsg) Informatik-Wirtschaft-Recht. Regulierung in der Wissensgesellschaft.

⁵² See also *Mattila* Comparative Legal Linguistics. Language of Law, Latin and Modern Lingua Franca, 2nd ed p. 75.

Lehtimaja Lauri Oikeutta eilen, tänään ja huomenna (Law yesterday, today and tomorrow), LM 2010: 223 (in Finnish).

Mattila, Heikki E. S. Comparative Legal Linguistics. Language of Law, Latin and Modern Lingua Franca, 2nd ed.

Saarenpää, Ahti – Pöysti, Tuomas (ed) Tietoturvallisuus ja laki: näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä (in Finnish). (1997)

Saarenpää, Ahti Perspectives on Privacy pp. 58 in Saarenpää (ed) Legal Privacy (2008).

Saarenpää, Ahti The Importance of Information Security in Safeguarding Human and Fundamental Rights in *Greenstein* Vem reglerar Informationssamhället? (2010) pp. 45.

Saarenpää, Ahti The Network Society and legal information. Some observations from the Nordic point of view. in www.hklii.hk/conference/paper/2D1.pdf

Saarenpää, Ahti Legal welfare and legal planning in the network society pp 47-69 in *Barzallo – Valdés – Reyes – Amoroso* (eds) XVI Congreso Iberoamericano de Derecho e Informática (2012).

Saarenpää, Ahti The Debtor Identity: Perspectives on Collecting Credit Information and Regulating its Use pp 457-468 in *Schweighofer – Kummer – Hötendorfer* (Eds.), Abstraktion und Applikation Tagungsband des 16. Internationalen Rechtinformatik Symposions IRIS 2013. Proceeding of the 16th International Legal Informatics Symposium.

Saarenpää, Ahti Data Protection in the Network Society – the exceptional becomes the natural pp 85-127 in *Galindo* (ed) El derecho de la sociedad en red, Lefis Series 14, Universidad de Zaragoza (2013)

Schweighofer, Erich – Gaster, Jens – Farrand, Benjamin (ed) KnowRight 2010. Knowledge Rights – legal, Societal and Related Technological Aspects. Österreichische Computer Gesellschaft (2010)

Schweighofer, Erich – Kummer, Franz – Hötendorfer, Walter (Eds.) Abstraktion und Applikation Tagungsband des 16. Internationalen Rechtinformatik Symposions IRIS 2013 Proceeding of the 16th International Legal Informatics Symposium.

Taeger, Jürgen – Wiebe, Andreas (Hrsg) Informatik-Wirtschaft-Recht. Regulierung in der Wissensgesellschaft. Festschrift für Wolfgang Kilian. Nomos 2004.

Verschuuren, Jonathan (ed) The Impact of Legislation: A Critical Analysis of Ex Ante Evaluation. Martinus Nijhoff Publishers (2009).

Wintgens. Luc J. (ed) Legislation in Context: Essays in Legisprudence. Ashgate (2007).

SURVEILLANCE NEEDS TRANSPARENCY AND DEMOCRATIC CONTROL

¹Walter Hötzenendorfer, ²Erich Schweighofer (Coordinators^{*})

¹Ph.D. researcher, ²Professor,

University of Vienna, Research Centre for Computers and Law

Schottenbastei 10-16/2/5, 1010 Vienna, AT

walter.hoetzenendorfer@univie.ac.at; erich.schweighofer@univie.ac.at; <http://rechtsinformatik.univie.ac.at>

Keywords: *Surveillance, Transparency, democratic control, Safe Harbor, European cloud, industrial espionage, Edward Snowden*

Abstract: *As a reaction to the worldwide surveillance techniques revealed by Edward Snowden, OCG Forum Privacy, a working group of the Austrian Computer Society (OCG), delivered the following opinion. The opinion was published on 27. August 2013 in the printed daily newspaper "Der Standard"; and was adopted as its official position by the OCG's executive board on 23. September 2013.*

Opinion of the Austrian Computing Society (OCG) on the global surveillance practices disclosed by Edward Snowden

The Internet does not forget. Most of our activities today leave digital footprints: smartphones reveal our whereabouts, surfing and searches tell about our interests. Information technology has reached a level of maturity that allows monitoring and analysing these activities and the communication of all citizens at the same time and almost everywhere. Edward Snowden's revelations about the most extensive monitoring activities in the history of mankind [1] show that it is essential for the survival of our democratic society to find a way to responsibly deal with these technical possibilities and bring back its use under democratic control.

If the existing technological capabilities are deployed and extensively proliferated for comprehensive monitoring of virtually all citizens regardless of whether a reasonable suspicion exists, this results in an abuse of these technologies, in an abuse of computer science. The Austrian Computer Society (OCG) strongly opposes this abuse and calls for a responsible use of information technology while respecting the fundamental rights to privacy and data protection. Publicity and training activities at all levels educating about the misuse of data and concerned fundamental rights are crucial for the purposes of developing a "digital civil society".

In some cases, the monitoring of suspicious persons may decisively contribute to the prevention or detection of crime. However, the monitoring of all with the aim of identifying or predicting a potentially suspicious behaviour should be rejected. The awareness of permanent monitoring and control means that people themselves even change legitimate behaviour and react with opportunistic adaptations to perceived expectations. The rights to

^{*} The text of this opinion was written in a joint effort by the persons who signed it (see below). This joint effort was coordinated by Walter Hötzenendorfer. The text was translated to English by Erich Schweighofer and Walter Hötzenendorfer.

freedom of expression and informational self-determination are thus disproportionately restricted, and consequently the political discourse and thus the political participation of the affected population – even without intentional control of political dissent using existing monitoring technologies. [2] Such control and other risks of abuse come however inherently with surveillance of the population, and the storage of large amounts of personal data.

In addition, monitoring activities inevitably lead to false positives: algorithms are not error-free, and “suspicious” actions often are commonplace and banal. Numerous cases of recent years show that unjustified suspicions of those concerned can lead to serious consequences. Not only this fact refutes the statement, “one who has nothing to hide, has nothing to fear.”

Even if an algorithm for identifying “suspicious behaviour” works so good that it produces only one false positive out of a million cases of harmless behaviours, it will result to numerous false positives in case of the analysis of the daily electronic activities of all Austrians alone. Moreover, those who have something criminal to hide will always find ways to effectively protect themselves from surveillance.

Neither enormous surveillance effort nor other measures can guarantee absolute security. If only for this reason, a balance must be found between security and privacy.

Thus, the OCG Privacy Forum calls for:

Transparency and democratic control: Democratic States must disclose their surveillance activities and must agree to their evaluation by computer scientists, lawyers, sociologists, etc. This should lead to a public debate on the powers of the security forces and intelligence services.

Disclosure: The Austrian government has to disclose Austria's international agreements with the U.S. and other countries, which reach far back into the era of the Cold War, and it must convincingly dispel the suspicion that its reluctance in reacting to the revelations by Edward Snowden is because Austria knew about the uncovered activities and Austrian authorities benefitted from them.

An effective replacement for the Safe Harbor Arrangement must be negotiated and concluded in order to ensure that European data protection standards are also valid for data transmitted to the United States; the present Arrangement is insufficient in this regard. EU Justice Commissioner Reding called Safe Harbor a “loophole”. [3]

An international treaty on the protection of fundamental rights on the internet and on the control of cyberwar must be negotiated and concluded.

Promotion of a European Cloud (“Airbus in the Clouds”): European initiatives must be started to achieve that in the future the most important services on the Internet are offered also by competitive European companies. As a consequence not only monopolies shall be eliminated and the European export economy shall be strengthened by utilising its location as an asset, but also citizens (of all countries) are provided with services that respect their privacy and that cannot be forced by public authorities to disproportionately disclose user data. This is urgently needed, as the cases of the e-mail providers Lavabit [4] and Silent Circle [5] show, that were voluntarily closed under pressure from the U.S. authorities (providers were not allowed to give more detailed information).

Evaluation: The software products and IT services used in the Austrian public administration need to be evaluated with respect to their security against surveillance measures. [6]

Measures against industrial espionage: Investigations and diplomatic steps have to be taken to prevent industrial espionage through surveillance by the state. [7]

Respect for the freedom of the press: This is a fundamental right also and especially for those journalists who make disproportionate surveillance measures known, thus contributing decisively to bring surveillance back under democratic control.

Signed: The members of the Privacy Forum of the Austrian Computer Society (OCG):

Walter Hötzenndorfer, co-chair
Dr. Christof Tschohl, co-chair
Reinhard Goebel, President of the OCG
Dr. Georg Becker
Prof. Dr. Gunter Ertl
Prof. Dr. Gerald Futschek
Prof. Dr. Georg Gottlob
Wolfgang Keck
Dr. Wolfram Proksch
Prof. Dr. Dr. Erich Schweighofer
Prof. Dr. Hannes Werthner

Working translation of 19/11/2013: Erich Schweighofer and Walter Hötzenndorfer

[1] Overview of the facts about the recent revelations:
<http://www.zeit.de/digital/datenschutz/2013-07/faq-nsa-skandal/komplettansicht>

[2] The examples which show that this occurs not only in authoritarian regimes are ranging from the Watergate scandal to the recent history and also to Austria.

[3] [http://europa.eu/rapid/press-release MEMO-13-710_en.htm](http://europa.eu/rapid/press-release_MEMO-13-710_en.htm)

[4] www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/ Lavabit had also been used by Edward Snowden.

[5] <http://www.forbes.com/sites/parmyolson/2013/08/09/e-mails-big-privacy-problem-qa-with-silent-circle-co-founder-phil-zimmermann/>

[6] It should be noted that in principle only open source software can be thoroughly investigated for the presence of so-called backdoors.

[7] Hints of economic espionage: http://www.washingtonpost.com/politics/kerry-to-face-questions-on-nsa-spying-during-south-america-trip/2013/08/12/afdab47e-0382-11e3-88d6-d5795fab4637_story.html

ÜBERWACHUNG BRAUCHT TRANSPARENZ UND DEMOKRATISCHE KONTROLLE

Walter Hötendorfer (Koordinator[†])

Projektassistent
Universität Wien, Arbeitsgruppe Rechtsinformatik
Schottenbastei 10-16/2/5, 1010 Wien, AT
Walter.Hoetendorfer@univie.ac.at; <http://rechtsinformatik.univie.ac.at>

Schlagwörter: *Überwachung, Transparenz, demokratische Kontrolle, Safe Harbor, Europäische Cloud, Wirtschaftsspionage, Edward Snowden*

Abstrakt: *Anlässlich der von Edward Snowden aufgedeckten weltweiten Überwachungspraktiken erarbeitete der Arbeitskreis Forum Privacy der OCG nachfolgende Stellungnahme, die am 27. August 2013 in der Printausgabe der Tageszeitung Der Standard erschien, und vom OCG-Präsidium am 23. September 2013 als offizielle Position der OCG angenommen wurde.*

Stellungnahme des OCG Forum Privacy zu den von Edward Snowden aufgedeckten weltweiten Überwachungspraktiken

Das Internet vergisst nicht. Die meisten unserer Aktivitäten hinterlassen heute digitale Spuren: Smartphones verraten unseren Aufenthaltsort, Surfen und Suchanfragen enthüllen unsere Interessen. Die Informationstechnologie hat einen Entwicklungsstand erreicht, der es ermöglicht, diese Aktivitäten und die Kommunikation aller Bürgerinnen und Bürger gleichzeitig und nahezu flächendeckend zu überwachen und auszuwerten. Edward Snowdens Enthüllungen über die umfangreichsten Überwachungsaktivitäten in der Geschichte der Menschheit [1] zeigen auf, dass es für den Fortbestand unserer demokratischen Gesellschaftsordnung unerlässlich ist, einen Weg zu finden, mit diesen technischen Möglichkeiten verantwortungsbewusst umzugehen und deren Einsatz wieder unter demokratische Kontrolle zu bringen.

Werden die vorhandenen technologischen Möglichkeiten ausufernd und unabhängig davon, ob ein konkreter Verdacht besteht, zur flächendeckenden Überwachung nahezu aller Bürgerinnen und Bürger eingesetzt, ist dies als Missbrauch dieser Technologien, als Missbrauch der Informatik zu werten. Das Forum Privacy der Österreichischen Computer Gesellschaft (OCG) spricht sich entschieden gegen diesen Missbrauch aus und fordert einen verantwortungsbewussten Umgang mit Informationstechnologie unter Wahrung der Grundrechte auf Privatsphäre und Datenschutz. Öffentlichkeitsarbeit und Bildungsmaßnahmen auf allen Ebenen, die über Datenmissbrauch und betroffene Grundrechte aufklären, sind dafür im Sinne der Entwicklung einer „digitalen Zivilgesellschaft“ eine entscheidende Voraussetzung.

Die Überwachung von verdächtigen Personen kann im Einzelfall entscheidend zur Verhinderung oder Aufklärung von Verbrechen beitragen. Doch die Überwachung aller mit dem Ziel, ein möglicherweise verdächtiges Verhalten festzustellen bzw. vorherzusagen, ist abzulehnen. Das Bewusstsein permanenter Überwachung und Kontrolle führt dazu, dass die

[†] Der Text dieser Stellungnahme wurde von den Personen, die ihn unterzeichnet haben, gemeinsam verfasst. Die Entstehung des Textes wurde von Walter Hötendorfer koordiniert.

Menschen selbst legitimes Verhalten verändern und mit opportunen Anpassungen an vermeintliche Erwartungshaltungen reagieren. Die Rechte auf freie Meinungsäußerung und informationelle Selbstbestimmung werden dadurch unverhältnismäßig eingeschränkt, was auch den politischen Diskurs und somit die politische Partizipation der Bevölkerung beeinträchtigt – selbst ohne bewusste Kontrolle politisch Andersdenkender mittels der vorhandenen Überwachungstechnologien. [2] Diese Kontrolle und andere Missbrauchsrisiken zählen ebenfalls zu den Gefahren der Überwachung der Bevölkerung und der Speicherung großer Mengen personenbezogener Daten.

Zudem führen Überwachungsmaßnahmen unweigerlich zu falschen Verdächtigungen: Algorithmen sind niemals fehlerfrei, die „verdächtigen“ Handlungen sind oft alltäglich und banal. Zahlreiche Fälle der vergangenen Jahre zeigen, dass zu Unrecht erfolgte Verdächtigungen für die Betroffenen folgenschwer sein können. Nicht nur dieser Umstand widerlegt die Aussage, „wer nichts zu verbergen hat, hat nichts zu befürchten.“

Selbst wenn ein Algorithmus zur Identifikation „verdächtigen Verhaltens“ so gut arbeitet, dass er nur in einem von einer Million Fälle harmloses Verhalten fälschlicherweise für verdächtig hält, führt dies alleine im Zuge der Analyse der elektronischen Aktivitäten aller Österreicherinnen und Österreicher täglich zu zahlreichen falschen Verdächtigungen. Jene, die etwas Kriminelles zu verbergen haben, werden zudem immer Möglichkeiten finden, sich vor Überwachung wirksam zu schützen.

Weder ungeheurer Überwachungsaufwand noch andere Maßnahmen können hundertprozentige Sicherheit gewährleisten. Schon allein aus diesem Grund muss eine Balance zwischen Sicherheit und Privatsphäre gefunden werden.

Das OCG Forum Privacy fordert daher:

- Transparenz und demokratische Kontrolle: Demokratische Staaten müssen ihre Überwachungsmaßnahmen offenlegen und dazu bereit sein, diese Maßnahmen von Informatikern, Juristen, Soziologen etc. evaluieren zu lassen; dies sollte in eine öffentliche Debatte über die Befugnisse der Sicherheitsbehörden und Geheimdienste münden.
- Die österreichische Bundesregierung muss völkerrechtliche Vereinbarungen Österreichs mit den USA und anderen Staaten, die teilweise bis weit in die Zeit des Kalten Krieges zurückreichen, offenlegen und glaubhaft die Vermutung ausräumen, dass ihre Reaktionen auf die Enthüllungen rund um PRISM deswegen so zurückhaltend ausfielen, weil sie von diesen Aktivitäten wusste und auch österreichische Behörden davon profitieren.
- Eine wirksame Nachfolgeregelung für das Safe-Harbor-Abkommen muss verhandelt und abgeschlossen werden, um das europäische Datenschutzniveau für in die USA übertragene Daten zu gewährleisten. Das gegenwärtige Abkommen erfüllt diesen Zweck nur unzureichend. Auch EU-Kommissarin Reding spricht von Safe Harbor als „Schlupfloch“. [3]
- Eine völkerrechtliche Vereinbarung zur Wahrung der Grundrechte im Internet und zur Kontrolle des Cyberwar muss verhandelt und abgeschlossen werden.
- Die Förderung einer europäischen Cloud („Airbus in the Clouds“): Es müssen Initiativen gestartet werden, um zu erreichen, dass in Zukunft die wichtigsten Dienstleistungen im Internet auch von konkurrenzfähigen europäischen Unternehmen angeboten werden. Dadurch sollen nicht nur Monopole ausgeschaltet und die europäische Wirtschaft durch Nutzung ihrer spezifischen Standortvorteile gestärkt, sondern vor allem den Bürgerinnen und Bürgern (aller Staaten) Dienste zur Verfügung

gestellt werden, die ihre Privatsphäre respektieren und nicht von Behörden zur unverhältnismäßigen Herausgabe von Nutzerdaten gezwungen werden können. Dies ist dringend nötig, wie die Fälle der E-Mail-Anbieter Lavabit [4] und Silent Circle [5] zeigen, die unter dem Druck der US-Behörden von ihren Betreibern freiwillig geschlossen wurden (genaueres durften die Betreiber dazu nicht bekannt geben).

- Die in der österreichischen Verwaltung eingesetzten Softwareprodukte und IT-Services müssen hinsichtlich deren Sicherheit gegenüber Überwachungsmaßnahmen evaluiert werden. [6]
- Ermittlungen und diplomatische Schritte sind einzuleiten, um Wirtschaftsspionage mittels staatlicher Überwachungsmaßnahmen zu unterbinden. [7]
- Die Achtung der Freiheit der Presse: Dieses Grundrecht gilt auch und insbesondere für jene Journalistinnen und Journalisten, die unverhältnismäßige Überwachungsmaßnahmen bekannt machen und dadurch entscheidend dazu beitragen, die Überwachung wieder unter demokratische Kontrolle zu bringen.

Gezeichnet: Die Mitglieder des Forum Privacy der Österreichischen Computer Gesellschaft (OCG):

Walter Hötzendorfer, Co-Leiter
Dr. Christof Tschohl, Co-Leiter
Reinhard Goebel, Präsident der OCG
Dr. Georg Becker
tit. ao. Univ.-Prof. Dr. Gunter Ertl
ao. Univ.-Prof. Dr. Gerald Futschek
O. Univ.-Prof. Dr. Georg Gottlob
Wolfgang Keck
Dr. Wolfram Proksch
ao. Univ.-Prof. DDr. Erich Schweighofer
Univ.-Prof. Dr. Hannes Werthner

[1] Überblick über die Fakten zu den Enthüllungen:
<http://www.zeit.de/digital/datenschutz/2013-07/faq-nsa-skandal/komplettansicht>

[2] Die Beispiele dafür, dass dies nicht nur in autoritären Regimen vorkommt, reichen vom Watergate-Skandal bis in die jüngere Geschichte und auch nach Österreich.

[3] http://europa.eu/rapid/press-release_MEMO-13-710_en.htm

[4] <http://www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/> Lavabit war auch von Edward Snowden verwendet worden.

[5] <http://www.forbes.com/sites/parmyolson/2013/08/09/e-mails-big-privacy-problem-qa-with-silent-circle-co-founder-phil-zimmermann/>

[6] Es ist darauf hinzuweisen, dass grundsätzlich nur Open-Source-Software umfassend auf das Vorhandensein von sogenannten Backdoors untersucht werden kann.

[7] Hinweise auf Wirtschaftsspionage: http://www.washingtonpost.com/politics/kerry-to-face-questions-on-nsa-spying-during-south-america-trip/2013/08/12/afdab47e-0382-11e3-88d6-d5795fab4637_story.html

PUBLIC VOICE IN PRIVACY GOVERNANCE: LESSONS FROM ENVIRONMENTAL DEMOCRACY¹

Dariusz Kloza²

Vrije Universiteit Brussel (VUB) – Research Group on Law, Science, Technology and Society (LSTS)
Pleinlaan 2, 1050 Elsene, Brussels, Belgium
dariusz.kloza@vub.ac.be; <http://www.vub.ac.be/LSTS>

Keywords: *Privacy, data protection, privacy impact assessment, environmental impact assessment, public participation, environmental democracy, access to information, participation in decision-making, access to justice, Aarhus Convention*

Abstract: Departing from a need to remedy the insufficient participation of stakeholders in the governance of privacy, and in particular in privacy impact assessment (PIA), this paper proposes the adaptation of the so-called environmental democracy, of which the 1998 Aarhus Convention is the most recent and most important formalisation, to the needs and reality of privacy, thus creating the “privacy democracy”. Such a framework would comprise three enforceable rights: to access privacy-related information, to take part in privacy-related decision-making in specific situations and to seek remedy should the two previous rights be violated. The experience of the functioning of environmental democracy would offer invaluable insight for the implementation of its privacy counterpart.

1. Introduction

Privacy will be to the information economy of the next century what consumer protection and environmental concerns have been to the industrial society of the 20th century.³

– Marc Rotenberg (1996)

Back in early 2006 I expressed the view that “Privacy is the new Green” – by which I meant that I thought advocates of a stronger approach to personal data privacy were regarded with the same bemused semi-tolerance as the ‘tree-hugging eco-warriors’ of preceding years. Ecological and sustainability issues are now, of course, squarely in the mainstream of both policy and public awareness, but privacy concerns are often still treated as if they were a niche lobbying interest, compelling only to conspiracy theorists, and those who, it is implied, must have “something to hide”.⁴

– Robin Wilton (2009)

The words of both Marc Rotenberg and Robin Wilton illustrate quite well at least two similarities between the approaches to the protection of privacy (including personal data) and that of the environment. Nowadays “the issue of privacy” has risen to prominence in many

¹ This paper is based on the research project PIAF (*Privacy Impact Assessment Framework for Data Protection and Privacy Rights*) (2011-2012), co-funded by the European Union under its Fundamental Rights and Citizenship Programme, <http://www.piafproject.eu>. The contents are the sole responsibility of the author and can in no way be taken to reflect the views of the European Commission.

² I wish to thank Paul De Hert, Colin J. Bennett, J. Peter Burgess, Armelle Gouritin, Anna Mościbroda, Irene Wieczorek and Barry Guihen for their useful comments. Paweł Baraniuk ably produced the bibliography.

³ Marc Rotenberg quoted in: Gleick, James, “Big Brother Is Us”, *New York Times*, 29 September 1996. <http://www.nytimes.com/1996/09/29/magazine/big-brother-is-us.html>

⁴ Wilton, Robin, *What's happened to PETs?*, Future Identity Ltd., Westbury, 27 September 2009, p. 5. <http://ftc.gov/os/comments/privacyroundtable/544506-00076.pdf>

aspects of life, and has received comparable attention to its environmental counterpart. Accordingly, the place of privacy protection on policy-makers' agendas – ideally – should be as high as that of the environment. These similarities suggest looking comparatively at the (legal) means that protect the environment and investigating whether any of them is useful for the (legal) protection of privacy.

Claims to look at other branches of law for an inspiration on how to protect best various aspects of privacy are not new *per se*. Such analyses have often focused on property law⁵ and competition law,⁶ among others, but it is environmental law that probably has attracted the most of attention. In the United States academic arena, Nehf (2003) was perhaps one of the first to propose an analogy between the protection of the environment and (informational) privacy, arguing that “in the modern digital world information privacy should be viewed as a societal value justifying a resolution in the public interest, much as we do environmental policy and other societal concerns.”⁷ Furthermore, assuming that “the privacy injuries of the Information Age are structurally similar to the environmental damage of smokestack era”, Hirsch (2006) claimed that second-generation environmental laws and policies “can serve as a model for protecting privacy in the digital age”. He understands the second-generation instruments as those initiatives that encourage the regulated parties *themselves* to choose the means by which they will achieve performance goals, as opposed to the „command-and-control” regulation in a form of prescriptive and uniform standards.⁸ He then has turned to the “specific lessons”, such as emission fees that could “readily be adapted for the purpose of reducing spam” and “regulatory covenants, pollution release and transfer registries, and government support for environmental management systems” that could be “adapted for the privacy field and used to protect personal information in the digital age”.⁹ In the European academic arena, De Hert – having analysed the case law of the European Court of Human Rights (ECtHR) related to the protection of “environmental health” – argued (2012) that “the current human rights framework requires States to organise solid decision-making procedures that involve the persons affected by technologies. ... Further case law is required to clarify the scope of the duty to study the impact of certain technologies and initiatives, *also outside the context of environmental health*”.¹⁰

In this paper I intend to advance these ideas and to examine how environmental law could further inspire the protection of privacy.¹¹ In particular, I would like to see how one of the

⁵ Cf. e.g. Purtova, Nadezhda, *Property Rights in Personal Data: A European Perspective*, Kluwer Law International, 2011.

⁶ Cf. e.g. Kloza, Dariusz, Anna Mościbroda, and Gertjan Boulet, “Improving Co-operation Between Data Protection Authorities: First Lessons from Competition Law,” *Jusletter IT. Die Zeitschrift Für IT Und Recht*, 2013, <http://jusletter-it.weblaw.ch/issues/2013/20-Februar-2013/2128.html>

⁷ Nehf, James, “Recognizing the Societal Value in Information Privacy”, *Washington Law Review*, Vol. 78, 2003, p. 5.

⁸ For the debate on classification of regulatory instruments, cf. e.g. Bronwen, Morgan, and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press, 2007, pp. 80-113.

⁹ Hirsch, Dennis, “Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law”, *Georgia Law Review*, Vol. 41, No. 1, 2006, pp. 8, 10-11, 23.

¹⁰ De Hert, Paul, “A Human Rights Perspective on Privacy and Data Protection Impact Assessments,” in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer Netherlands, 2012, pp. 70-74 (emphasis added). Cf. also section 4.3.

¹¹ For the conceptualisation and legal construction of both privacy and data protection as well as the relationship between these two, cf. Gutwirth, Serge, Michael Friedewald et al., *Legal, social, economic and ethical conceptualisations of privacy and data protection*, Deliverable D1 of the PRESCIENT project [Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment], Karlsruhe, March 2011, p. 8. <http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf>

aspects of environmental law, i.e. the framework for public participation in environmental decision-making, could inspire the strengthening of public voice in decision-making in privacy matters and especially in privacy impact assessment (PIA). This exercise aims to improve the level of the protection of the right to privacy by analysing a potential new means of protection.¹²

There are many points where the governance of privacy meets the governance of environment and perhaps the most important one is the use of human rights language. In many jurisdictions privacy is explicitly considered a human right. However, this is not necessarily a case with “environment”, which has not (yet) received such recognition internationally, but a human rights machinery is often used to obtain some protection thereof (cf. *infra*, at 4.3).

From a technical viewpoint, another “meeting point” in the governance of both fields is the use of impact assessments.¹³ In other words, in both fields impact assessments are employed as a tool aimed primarily at better decision-making. Such assessments emerged precisely in the field of environment during 1960s in the United States,¹⁴ but lately they have been gaining growing worldwide importance in the field of privacy. To that end, the concept of PIA came to the light and matured during the period 1995–2005.¹⁵ This increased interest in PIA has been predominantly rooted in public distrust of emerging technologies in general, by the robust development of privacy-invasive tools, by a belated public reaction against the increasingly privacy-invasive actions of public authorities and private sector, as well as by a natural progress of rational management techniques.¹⁶ PIA has shifted the attention from reactive measures towards more anticipatory instruments in the belief in the rational of an “ounce of prevention”, i.e. in trying to prevent privacy abuses before they occur.¹⁷

Crucial to the success of any impact assessment is the meaningful participation of stakeholders, i.e. those to be affected and those likely to be affected by the envisaged project, initiative, etc. as well as those who have any interest therein or their representatives, e.g. NGOs. Strongly linked to fundamental rights, to the concept of democracy and to corporate governance, public participation brings benefits for decision-making in both public and private sectors. Therefore methodologies for impact assessments often acknowledge the need for stakeholders’ participation.¹⁸ So does the European Commission’s *Smart Regulation*

¹² This paper is situated well in the debate on the role of the “tools” for protection of privacy, such as Privacy by Design, Privacy by default, Privacy Enhancing Technologies (PETs) and privacy impact assessments (PIAs).

¹³ There are many definitions of the notion of impact assessment as well as many types thereof. Put simply, an impact assessment is a tool that aims to support decision-making. It is a process that prepares evidence for decision-makers on the advantages and disadvantages of possible options by assessing their potential impact. Impact assessment emerged in the fields such as environment, regulation, health and fundamental rights, among others. European Commission, *Impact Assessment*, 2012. http://ec.europa.eu/governance/impact/index_en.htm

¹⁴ Noble, Bram F., *Introduction to Environmental Impact Assessment: A Guide to Principles and Practice*, 2nd ed., Oxford University Press, 2009, p. 2.

¹⁵ Privacy impact assessment (PIA) is usually defined as a process for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise the negative impacts. De Hert, Paul, Dariusz Kloza, David Wright, *Recommendations for a privacy impact assessment framework for the European Union*. Deliverable D3 of the PIAF project [A privacy impact assessment framework for data protection and privacy rights], Brussels, 2012, p. 5. http://www.piafproject.eu/ref/PIAF_D3_final.pdf

¹⁶ Clarke, Roger, „Privacy Impact Assessment: Its Origins and Development”, *Computer Law and Security Review*, Vol. 25, No. 2, 2009, pp. 123-135. <http://www.rogerclarke.com/DV/PIAHist-08.html>

¹⁷ Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate Publishing, Limited, 2003, p. 204.

¹⁸ International Finance Corporation, *Guide to Human Rights Impact Assessment and Management*, Washington, 2010, http://www.guidetohriam.org/app/images/secure/GuidetoHRIAM_v13_LR.pdf; International Finance Corporation, *Introduction to Health Impact Assessment*, Washington, 2009,

policy¹⁹ as well as the Commission's *Impact Assessment Guidelines*.²⁰ Assessors are assisted by a number of textbooks discussing techniques for stakeholders' participation.²¹ However, as it will be demonstrated *infra*, existing PIA frameworks as well as the current practice of PIA with regard to such participation leave much to be desired.

In order to remedy the problem of insufficient public participation in PIA and thus to strengthen public voice in privacy decision-making, a lesson might be drawn from environmental law. Acknowledging that "environmental issues are best handled with the participation of all concerned citizens",²² this branch of law has developed a comprehensive framework for environmental procedural rights. The so-called environmental democracy encompasses three rights: access to environmental information, participation in decision-making on specific activities and access to justice. All of these rights are interconnected: put simply, access to environmental information is a prerequisite for a meaningful participation in decision-making and access justice is meant to remedy a violation of any of the two previous rights. The concept of environmental democracy can comprise various means to exercise these rights, of which environmental impact assessment (EIA) is the most important in practice; others include e.g. standalone access to information and its dissemination. The most recent formalisation of this idea in Europe is the 1998 Aarhus Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters.²³ A similar framework is provided in the 1991 Espoo Convention on Environmental Impact Assessment in a Transboundary Context (Arts 3-5)²⁴ and in 2003 African Convention on the Conservation of Nature and Natural Resources (Art. XVI).²⁵ Elements of this framework are present in numerous jurisdictions worldwide.²⁶

Taking as a starting point the arguments that public participation is crucial for decision-making, and for impact assessments in particular, as well as that the *status quo* of such participation in PIA still requires improvement, this article argues that it is worth to consider the adaptation of the concept of environmental democracy to the governance of privacy in order to strengthen the public voice in the latter. I shall proceed as follows. In the second

http://www1.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/ifc+sustainability/publications/publications_handbook_healthimpactassessment_wci_1319578475704

¹⁹ European Commission, *EU Regulatory Fitness*, Brussels, 12 December 2012, COM(2012) 746 final.

²⁰ European Commission, *Impact Assessment Guidelines*, Brussels, 15 January 2009, SEC(2009) 92; cf. further Art 2 of the Protocol (No. 2) on the application of the principles of subsidiarity and proportionality, attached to the EU Treaties.

²¹ Cf. e.g. Organisation for Economic Cooperation and Development, *Stakeholder Involvement Techniques*, Paris, 2004. <http://www.oecd-neo.org/rwm/reports/2004/nea5418-stakeholder.pdf>; Taschner, Stefan and Matthias Fiedler, *Stakeholder Involvement Handbook*, Deliverable D2.1 of the AENEAS project [Attaining Energy Efficient Mobility in an Ageing Society], 21 April 2009. http://www.aeneas-project.eu/docs/AENEAS_StakeholderInvolvementHandbook.pdf; Neil Jeffery, *Stakeholder Engagement: A Road Map to Meaningful Engagement*, Doughty Centre, Cranfield School of Management, April 2009. http://www.som.cranfield.ac.uk/som/dinamic-content/think/documents/CR_Stakeholder.pdf

²² United Nations, *Rio Declaration on the Environment and Development*, 1992, Principle 10. <http://www.un.org/documents/ga/conf151/aconf15126-1annex1.htm>

²³ Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, adopted on 25 July 1998 in Aarhus, Denmark (hereinafter: Aarhus Convention). The Convention was prepared under the auspices of the United Nations Economic Commission for Europe (UNECE). As of April 2013, there were 47 Parties to the Convention, including all Member States of the European Union. Cf. UNECE, *Public Participation*, 2013. <http://www.unece.org/env/pp/ratification.html>

²⁴ The Convention on Environmental Impact Assessment in a Transboundary Context, adopted on 25 February 1991 in Espoo, Finland (hereinafter: Espoo Convention).

²⁵ The African Convention on the Conservation of Nature and Natural Resources, adopted on 11 July 2003 in Maputo, Mozambique. <http://www.tematea.org/?q=node/6416>.

²⁶ Noble, op. cit., p. 7.

section, I will overview the concept of and the rationale for public participation in decision-making. In the third section, I will analyse how the public nowadays is involved in the process of PIA. Next, in the fourth section, I shall overview the three procedural rights that constitute the environmental democracy. I shall pay special attention to the state's obligation to collect and disseminate environmental information. By analysing the relevant case law of the ECtHR I shall analyse the role of the environmental procedural rights in protecting fundamental rights in Europe. Furthermore, since many courts and extra-judicial bodies on various levels in Europe have dealt with environmental democracy, thus offering invaluable insight into its practical application, I shall analyse for that purpose the example of selected case law of the European Court of Justice (ECJ).²⁷ I will conclude, in the fifth section, by proposing the adaptation of the framework for environmental democracy to the needs and reality of privacy. Additionally, I shall analyse the most evident limitations that such an adaptation might face as well as some possibilities for further research. In this paper I will take the legal perspective: I shall explore all these issues from the human rights viewpoint in the European context.

2. Why should the public participate in decision-making?

Sustainable management of resources and ecosystems should be shaped by those who are most at risk. ... The core issues involved are procedural fairness – allowing people to be part of the process – and community empowerment – enabling people to take an active role in decision affecting their lives.²⁸

– Jona Razzaque (2012)

... a survey ... identified eight participation functions: (1) Give information to citizens; (2) Get information from and about citizens; (3) Improve public decisions and programs; (4) Enhance acceptance of public decisions and build consensus; (5) Supplement public agency work; (6) Change political power patterns and power allocations; (7) Protect individual and minority group rights and interests; and (8) Delay or avoid making difficult public decisions.²⁹

– Advisory Committee on Intergovernmental Relations (1980)

We have learnt that it is necessary with major technologies to ensure that the debate takes place 'upstream', as new areas emerge in the scientific and technological development process.³⁰

– Lord Sainsbury, UK Science Minister (2004)

Defined most broadly, public participation is a process by which concerns, needs and values of both the public at large and of individuals³¹ are incorporated into governmental and

²⁷ The selection of the cases under scrutiny does not come from a systematic analysis of all „environmental” cases in both Courts, but from an attempt to illustrate only the main points.

²⁸ Razzaque, Jona, “Information, public participation and access to justice in environmental matters”, in: Alam, S., Bhuyian, J., Chowdhury, T. and Techera, E. (eds.), *Routledge Handbook of International Environmental Law*. Routledge, 2012, p. 138.

²⁹ A survey conducted by Advisory Committee on Intergovernmental Relations, cited in: Popović, Neil A.F., „The Right To Participate In Decisions That Affect The Environment”, *Pace Environmental Law Review*, Vol. 10, 1993, p. 685.

³⁰ [UK] Department of Trade and Industry, „Nanotechnology offers potential to bring jobs, investment and prosperity – Lord Sainsbury”, press release, London, 29 July 2004. <http://www.voyle.net/Nano%20Debate/Debate2004-0017.htm>

³¹ Despite the environment being predominantly a collective interest (cf. Francioni, Francesco, “International Human Rights in an Environmental Horizon,” *European Journal of International Law*, Vol. 21, No. 1, 2010, pp. 41–55), public participation is a way to advocate the interests not only of the public at large, but also of individuals. As the ECtHR underlined on numerous occasions, in the field of environment, “the decision-making process leading to measures of interference must be fair and must afford due respect to the interests

corporate decision-making.³² It might go as far as to include individuals making and implementing decisions directly in ways that are largely or even entirely independent of public authorities. In a narrow sense, it is an organized process adopted by public authorities or private sector organizations to engage the public in assessment, planning, decision-making, management, monitoring and evaluation. Often the role of the public is advisory and in this sense public participation constitutes an immediate precursor to decision-making.³³ The public might range from organised interests to experts to just individuals; these people are most often external to public authorities or private sector organisations.

Much ink has been spilled over the rationale for public participation in decision-making, but the main reasons have to do with international fundamental rights law and with the concept of democracy, including the place of science in a democratic society. For the private sector in particular such participation is linked to the concept of corporate responsibility. Summing up, the rationale for public participation follows to some extent the logics of the famous slogan “no taxation without representation”. In any case, its most important benefit is the improvement of decision-making quality.

The first argument sees public participation in decision-making as a requirement derived from international fundamental rights.³⁴ The right “to take part in the government of his country, directly or through freely chosen representatives” is foreseen in Art. 21 of the Universal Declaration of Human Rights (1948). Similarly, Art. 25 of the International Covenant on Civil and Political Rights (1966) foresees that “every citizen shall have the right and the opportunity ... to take part in the conduct of public affairs, directly or through freely chosen representatives”. So does Art. 29 of the American Convention on Human Rights.³⁵ The UN Human Rights Committee further elaborated that “citizens also take part in the conduct of public affairs by exerting influence through public debate and dialogue with their

safeguarded to the individual by Article 8”. Therefore, “in a case involving decisions affecting environmental issues” the Court would “scrutinise the decision-making process to ensure that due weight has been accorded to the interests of the *individual*” (emphasis added). ECtHR, *Hardy and Maile v. the United Kingdom*, Judgement of 14 February 2012, Application No. 31965/07, §§ 217-219; *Giacomelli v. Italy*, Judgement of 2 November 2006, Application No. 59909/00, §§ 79-82; *Taşkın and Others v. Turkey*, Judgement of 10 November 2004, Application No. 46117/99, §§ 115-118. Furthermore, the ECJ struck a similar chord: “Moreover, the requirement that the cost should be ‘not prohibitively expensive’ pertains, in environmental matters, to the observance of the right to an effective remedy enshrined in Article 47 of the Charter of Fundamental Rights of the European Union, and to the principle of effectiveness, in accordance with which detailed procedural rules governing actions for safeguarding an *individual’s* rights under European Union law must not make it in practice impossible or excessively difficult to exercise rights conferred by European Union law” (emphasis added). ECJ, *The Queen, on the application of David Edwards and Lilian Pallikaropoulos v Environment Agency and Others*, Judgement of 11 April 2013, Case C-260/11, § 33. AG Kokott observed, in the same case, that “taking the public interest into account does not, however, rule out the inclusion of any individual interests of claimants. ... the presence of individual interests cannot prevent all account being taken of public interests that are also being pursued. For example, the individual interests of a few people affected by an airport project cannot, upon assessment of the permissible costs, justify disregard for the considerable public interest in the case which in any event stems from the fact that the group of those affected is very much wider.” ECJ, *Opinion of Advocate General Kokott*, Case C-260/11, §§ 45-46.

³² Creighton, James L., *The Public Participation Handbook: Making Better Decisions Through Citizen Involvement*, Wiley, 2005, p. 7.

³³ Cf. Dietz, Thomas, and Paul C. Stern, “Introduction,” in Thomas Dietz and Paul C. Stern, *Public Participation in Environmental Assessment and Decision Making*, National Academy of Sciences, 2008, pp. 11-12.

³⁴ Cf. also section 4.3 *infra*. For the rationale of the right to participate, cf. Brownsword, Roger, and Morag Goodwin, *Law and the Technologies of the Twenty-First Century: Text and Materials*, Cambridge University Press, 2012, pp. 248-252.

³⁵ By contrast, Art 3 of the Additional Protocol to the European Convention on Human Rights (1950) is limited to the elections to the legislature.

representatives or through their capacity to organize themselves.”³⁶ Since a meaningful participation requires access to relevant information, the free communication of information and ideas about public and political issues is essential.³⁷ Thus this participation is “supported by ensuring freedom of expression, assembly and association”.³⁸ Consequently, the disclosure of relevant information enhances transparency of decision-making and constitutes a prerequisite for accountability.

Second, public participation is intrinsic to democratic governance. In particular, from the deliberative democracy viewpoint, the idea of legitimate law making issues from the public deliberations of citizens and not merely from elections.³⁹ Deliberative democracy constitutes a form of government in which free and equal citizens (and their representatives) justify decisions in a process in which they give one another reasons that are mutually acceptable and generally accessible, with the aim of reaching conclusions that are binding in the present on all citizens but open to challenge in the future.⁴⁰ In practical terms, deliberative democracy is a way to supplement traditional forms of democracy by advocating for the involvement of citizens in decision-making in ways other than electoral.⁴¹ In the words of della Porta, “democracy cannot rely only upon checks every four or five years at elections; there must be other ways of controlling those in power. We cannot ask people just to vote – they need to participate”.⁴²

Hildebrand also highlights the place of science in democracy:

Taking democracy serious means that the scientists and engineers that produce hybrids like RFID systems, genetic tests or technologically enhanced soldiers should be obligated to present their case to the public that is composed of those that will suffer or enjoy the consequences. ... When funding and developing specific technologies these publics should have the opportunity to voice their opinion, co-determining the direction of research as well as the introduction of such artifacts into everyday life infrastructures. Different types of technology assessment (TA) have been developed to involve lay persons into the early stages of technological design ... often entailing citizen participation.⁴³

Third, there is a strong business case for public participation, as it constitutes an integral element of corporate responsibility. A company should be aware of, and responsive to, the demands of its stakeholders, including employees, customers, suppliers and local communities.⁴⁴ Furthermore, by engaging stakeholders a company can reduce costs, gain public trust and support, avoid activism and escape negative public reaction or loss of reputation, among others.

³⁶ Human Rights Committee, *General Comment No. 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service*, 12 July 1996, CCPR/C/21/Rev.1/Add.7, at 8.

³⁷ Jayawickrama, Nahil, *The Judicial Application of Human Rights Law: National, Regional and International Jurisprudence*, Cambridge University Press, 2002, p. 793.

³⁸ Human Rights Committee, *op. cit.*, at 8.

³⁹ Bohman, James F., and William Rehg, *Deliberative Democracy: Essays on Reason and Politics*, Cambridge 1997, p. ix.

⁴⁰ Gutmann, Amy and Dennis Thompson, *Why Deliberative Democracy?*, Princeton, 2004, p. 7.

⁴¹ Tanasescu, Irina, *The European Commission and interest groups. Towards a deliberative interpretation of stakeholder involvement in EU policy-making*, Brussels, 2007, p. 15.

⁴² della Porta, Donatella, *Can democracy be saved? Representation, Participation and Deliberation*, paper presented at conference *Democratic Representation in Crisis: what kinds of theories for what kinds of research, and to what ends?*, Florence, 9-10 April 2013, quoted in: European University Institute, *Citizens respond to crisis by reshaping democracy, press release*, Florence, 18 April 2013. <http://www.eui.eu/News/2013/04-18-Citizensrespondtocrisisbyreshapingdemocracy.aspx>

⁴³ Hildebrandt, Mireille, “Legal and Technological Normativity: More (and Less) than Twin Sisters,” *Techné*, Vol. 12, No. 3, 2008. http://works.bepress.com/mireille_hildebrandt/13

⁴⁴ Blowfield, Michael, and Alan Murray, *Corporate Responsibility*, Oxford University Press, 2011, pp. 207.

The fourth and the last argument links those three previous: public participation contributes to informed decision-making with a view to improve its quality. In particular, engaging stakeholders helps to discover risks and impacts that might not otherwise be considered. It is a way to gather fresh input on the perceptions of the severity of risks and on possible measures to mitigate them.⁴⁵ In complex and uncertain situations, it can overcome the incompleteness of scientific knowledge as the management of risks cannot solely be based upon technical knowledge.⁴⁶ In other words, the public may have information, ideas, views or values that had not been previously considered or had been regarded as relatively minor.⁴⁷ The public may also be able to suggest alternative courses of action to achieve the desired objectives or may have some suggestions for resolving complex issues.⁴⁸

Against the foregoing, critics often worry that participation in practice may not achieve the goals articulated in theory and may actually impede good decision-making. They offer three basic arguments: that the costs (i.e. time, money and manpower) are not justified by the benefits, that the public is ill-equipped to deal with the complex nature of analyses that are needed for good assessments and decisions, and that participation processes seldom achieve equity in process and outcome.⁴⁹ Furthermore, potential stakeholders might lack interest, whereas some with strong but specific interests might dominate the agenda.⁵⁰ Others argue that participatory processes tend to experience a set of pathologies that range from paralysis by endless deliberations to reaching only trivial results when trying to accomplish a consensus among stakeholders with conflicting values and interests.⁵¹

Despite the strong case for public participation in decision-making, the *status quo* of such participation in PIA, as it will be demonstrated in the following section, leaves much to be desired.

3. How does the public voice come to the fore in privacy impact assessment?

... opinions and feedback from relevant stakeholders ... should be appropriately considered as part of the PIA review of potential concerns and issues. Consultations should be appropriate to the scale, scope, nature, and level of the RFID Application.⁵²

– *Privacy and Data Protection Impact Assessment Framework for RFID Applications* (2011)

⁴⁵ Wright, David, “The State of the Art in Privacy Impact Assessment,” *Computer Law & Security Review*, Vol. 28, No. 1, 2012, p. 58.

⁴⁶ This follows the logic of the precautionary principle, well established in environmental law. According to the 15th principle of the 1992 Rio Declaration (op. cit.): “where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation.” Cf. e.g. Wright, David, Raphael Gellert, Serge Gutwirth, and Michael Friedewald, “Minimizing Technology Ricks with PIAs, Precaution, and Participation,” *IEEE Technology and Society Magazine*, Vol. 30, No. 4, 2011, pp. 47–54.

⁴⁷ Wright, op. cit., p. 58.

⁴⁸ Wright, David and Emilio Mordini, “Privacy and Ethical Impact Assessment”, in Wright and De Hert, op. cit., p. 397.

⁴⁹ Dietz, Thomas, and Paul C. Stern, “The Promise and Perils of Participation,” in Thomas Dietz and Paul C. Stern, *Public Participation in Environmental Assessment and Decision Making*, National Research Council, 2008, pp. 33-34.

⁵⁰ Owens, Phil, *Sediment Management at the River Basin Scale*, Elsevier Science, 2007, p. 207.

⁵¹ Dietz and Stern, op. cit., pp. 51-66.

⁵² *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, Brussels, 12 January 2011. http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf. The Framework is based on the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by Radio-Frequency Identification, Brussels, 12 May 2009, C(2009) 3200.

Where processing operations present specific risks to the rights and freedoms of data subjects ... the controller ... shall carry out an assessment of the impact of the envisaged processing operations on the protection of personal data ... The controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.⁵³

– *Proposal for ... General Data Protection Regulation* (2012)

The history of PIA in the European Union (EU) legal order⁵⁴ started in 2009 when the European Commission issued a recommendation on safeguarding privacy and personal data in Radio-Frequency Identification (RFID) applications.⁵⁵ The Commission suggested developing of a PIA framework for such applications, a task that was accomplished almost two years later. January 2012 saw tabling of a proposal for the General Data Protection Regulation,⁵⁶ which – if turned into law – would foresee a mandatory data protection impact assessment (DPIA).⁵⁷ It is apparent from the two quotations above that both frameworks opt for engaging stakeholders in the PIA process. From a global perspective, however, only few PIA frameworks, be it hard-law or soft-law, explicitly provide for stakeholders' involvement. A study on PIA indicated that, apart from the EU, only four out of thirteen examined frameworks worldwide clearly foresee the participation of stakeholders: Australia, the Australian state of Victoria, Ireland and the United Kingdom.⁵⁸

In practice, the final PIA reports often fail to acknowledge the importance of the stakeholders' consultation or give it limited berth. At other times, details on such consultations are lacking or the stakeholders are not adequately identified.⁵⁹ For example, Canadian PIAs seldom involve public consultation, opinion polling or other means of gauging the privacy values of the public. The end product tends to resemble a compliance checklist and does not require documentation of deliberations.⁶⁰

Furthermore, the public has often difficulties in benefiting from reports of PIAs actually carried out or – at least – from summaries thereof. For instance, the Canadian federal audit of PIAs carried out revealed that only a minority of the institutions audited were regularly posting and updating the results of PIA reports to their external web sites. Just as public reporting on PIAs was lacking in completeness, so too was it lacking in quality. Despite the government's recommendation that PIA summaries describe the privacy impacts of all new

⁵³ European Commission, *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)*, Brussels, 25 January 2012, COM(2012) 11 final.

⁵⁴ In the Member States of the European Union it started in 2007 when the Information Commissioner's Office (ICO) published its first PIA Handbook. The 2nd edition (2009) does provide for stakeholders' consultation. ICO, *Privacy Impact Assessment Handbook*, Wilmslow, Cheshire, UK, Version 2.0, June 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

⁵⁵ European Commission, *Recommendation...*, op. cit., fn. 52.

⁵⁶ European Commission, *Proposal...*, op. cit., fn. 53.

⁵⁷ For the sake of comparison, the modernisation of the Council of Europe's Convention 108 also introduces privacy risk management but it offers no explicit provision on public participation [Art 8bis(2)]. Council of Europe, *Modernisation of Convention 108*, Strasbourg, 29 November 2012, T-PD(2012)4Rev3_en. [http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD\(2012\)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf](http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD(2012)4Rev3E%20-%20Modernisation%20of%20Convention%20108.pdf)

⁵⁸ Wright, David, Kush Wadhwa, Paul De Hert, and Dariusz Kloza (eds.), *PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights*. Deliverable D1 of the PIAF project, 21 September 2011, pp. 187-188. http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf. Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents," *International Data Privacy Law*, Vol. 1, No. 2, 2011, pp. 111-120.

⁵⁹ Wright, Wadhwa, De Hert, Kloza, op. cit., p. 193.

⁶⁰ Bayley, Robin, and Colin Bennett, "Privacy Impact Assessments in Canada," in Wright and De Hert, op. cit., p. 183.

programs and the measures taken to mitigate them, none of the reviewed departmental summaries contained more than a simple project description and “privacy disclaimer”. Privacy issues were rarely described and action plans were generally missing.⁶¹

From a policy perspective, the majority of EU data protection authorities do not support compulsory stakeholders’ consultation in the PIA process. When asked about the optimum PIA policy for the EU, the common view expressed is that external stakeholder engagement is a matter that should be left to either individual organisations or to the Member States to determine. Only one such authority sees stakeholder engagement as indispensable while other authority argues that “such an obligation makes sense especially for products and services that will necessarily affect a specific category of people in everyday life: employees, hospital patients, public transport users, etc.”⁶² (In a broader sense, observed could be a tendency to oppose any external dimension of PIA, i.e. any form of engaging external entities in the PIA process, be it third-party audit, central registry of PIAs actually carried out or filling in PIA reports to the competent supervisory authority.)⁶³

It is therefore apparent that the notion of public participation in the process of PIA is not yet commonly accepted and requires further encouragement. A “wish-list” here would include a widely practiced PIA, supported by public authorities (including data protection authorities and privacy commissioners) and conducted on the basis of methodologies in which stakeholders’ participation is a core element. In other words, a framework in which the stakeholders are identified, appropriately informed about the envisaged measure, properly heard and their views taken into consideration. Furthermore, if they are not informed or heard in a correct way, they should be able to remedy that. Such methodologies should be adequately detailed and accompanied by practical guidance. To that end, a valuable lesson can be learnt from environmental law. In the next section I will discuss procedural environmental rights and analyse how these rights can be of inspiration for improving public participation in privacy governance and in particular in PIA.

4. How does public participation come to the fore in environmental law?

4.1. The concept of environmental democracy

Environmental issues are best handled with the participation of all concerned citizens, at the relevant level. At the national level, each individual shall have appropriate access to information concerning the environment that is held by public authorities, including information on hazardous materials and activities in their communities, and the opportunity to participate in decision-making processes. States shall facilitate and encourage public awareness and participation by making information widely available. Effective access to judicial and administrative proceedings, including redress and remedy, shall be provided.⁶⁴

– *Rio Declaration on the Environment and Development* (1992)

Principle 10 of the 1992 Rio Declaration, quoted above, is an encapsulation of the view that procedural rights are an essential part of environmental regulation.⁶⁵ An underlying premise is

⁶¹ Example taken from Stoddart, Jennifer, *Auditing privacy impact assessments: the Canadian experience*, Wright and De Hert, op. cit., p. 434.

⁶² Hosein, Gus, and Simon Davies, *Empirical research of contextual factors affecting the introduction of privacy impact assessment frameworks in the Member States of the European Union*, Deliverable D2 of the PIAF project, August 2012, pp. 16, 35, 69. http://www.piafproject.eu/ref/PIAF_deliverable_d2_final.pdf

⁶³ Hosein and Davies, op. cit., pp. 11-20.

⁶⁴ United Nations, *Rio Declaration...*, principle 10, op. cit.

⁶⁵ Douglas-Scott Sionaidh, “Environmental Rights: Taking the Environment Seriously”, in Gearty, C.A., and A. Tomkins, *Understanding Human Rights*, Continuum International Publishing Group, Limited, 1996, pp. 436.

that these rights should “contribute to the protection of the right of every person of present and future generations to live in an environment adequate to his or her health and well-being”.⁶⁶ In practice, a procedural approach provides environmental protection by way of democracy, i.e. by ensuring that those who have to live with the consequences of environmental degradation will be able to have their say in *how*, *if* and *when* it should occur.⁶⁷ Such an approach is also an attempt to remedy the situation of the “silent environment” because – as Krämer puts it – the environment is an “interest without a group”.⁶⁸ In result, developed has been the so-called environmental democracy, i.e. an advanced, three-pillar framework for environmental procedural rights, providing for the rights to (1) access to information, (2) participation in decision-making on specific activities, and (3) effective access to justice.

The 1998 Aarhus Convention formalised the above-mentioned environmental procedural rights.⁶⁹ In the Convention, the first pillar of environmental democracy, i.e. access to information (Arts 4-5), comes into two forms: “passive”, i.e. where public authorities provide information on request, and “active”, i.e. where public authorities gather, publish and promote information widely, making it easy accessible and affordable for all. For “passive” access, the Convention stipulates that every individual and every legal person has a right to access environmental information,⁷⁰ in the form requested, without stating any interest and without undue delay. Public authorities may refuse the request for environmental information on the grounds of confidentiality of commercial and industrial information, intellectual property rights and personal data, among others. These grounds for refusal shall be interpreted in a restrictive way. For the “active” access, the Convention requires public authorities to collect and disseminate environmental information; special emphasis is paid to the digital form of dissemination.

The second pillar, i.e. participation in decision-making, offers a right to take part therein by receiving information and providing comments (Arts 6-8). However, public participation is required only for planned activities that, generally speaking, have a “significant effect on the environment”. An extensive list of such activities is provided in Annex I to the Convention. Yet nothing precludes the parties to the Convention to extend this list in their jurisdictions. Furthermore, the second pillar’s *ratione personae* is limited to the so-called public concerned, i.e. those affected or likely to be affected as well as those who have an interest therein. Nevertheless, the Convention extends this scope to non-governmental organisations promoting environmental protection that meet any requirements under national law. The

⁶⁶ Art 1 of the Aarhus Convention, op. cit.

⁶⁷ Sionaidh, op. cit., pp. 436-437.

⁶⁸ Krämer, Ludwig, *Access to justice in environmental matters, in particular by NGOs* [manuscript]. Cf. Stone, Christopher D., „Should Trees Have Standing – Toward Legal Rights for Natural Objects”, *South California Law Review*, Vol. 45, 1972; Stone, Christopher, *Should Trees Have Standing? Law, Morality, and the Environment*, Oxford University Press, 2010; Sama, Linda M., Stephanie A. Welcomer, and Virginia V. Gerde, “Who Speaks for the Trees? Invoking an Ethic of Care to Give Voice to the Silent Stakeholder,” in Sanjay Sharna and Mark Starik, *Stakeholders, The Environment And Society*, Edward Elgar Publishing, 2004, pp. 140–161.

⁶⁹ Cf. also Hart, David, “Aarhus for real beginners”, *UK Human Rights Blog*, 12 October 2013. <http://ukhumanrightsblog.com/2013/10/12/aarhus-for-real-beginners/>

⁷⁰ Art 2(3) of the Aarhus Convention defines environmental information as any information in written, visual, aural, electronic or any other material form on (1) the state of elements of the environment and the interaction among them, (2) factors and activities or measures affecting or likely to affect the elements of the environment as well as cost-benefit and other economic analyses and assumptions used in environmental decision-making, and (3) the state of human health and safety, conditions of human life, cultural sites and built structures, inasmuch as they are or may be affected by the state of the elements of the environment or, through these elements, by the factors, activities or measures affecting the environment.

Convention requires that the procedures for such participation should include reasonable time frames and, eventually, due account must be taken of the outcome thereof.

For the third pillar, i.e. access to justice (Art. 9), anyone whose request for information has been ignored, anyone who believes such a request has been wrongly treated, or whose rights to participate in decision-making has not been respected, has a right to seek justice (Art. 9).

The Aarhus Convention is characterised by taking a rights-based approach, by affording minimum standards, by compliance monitoring and by providing a high level of prescriptiveness. The rights to access information and to participate in decision-making are enforceable, safeguarded by the right to seek justice. A party to the Convention can introduce measures providing for broader access to information, more extensive public participation in decision-making and wider access to justice than required by the Convention. On the basis of Art. 15, the Convention Compliance Committee was established to monitor observance, examining compliance on its own initiative or by accepting submissions from the parties and from the Secretariat to the Convention as well as from the public.⁷¹ The Convention spells out all three rights in a very detailed way with a view of their easier application and better observance. To illustrate the last point, let me quote in its entirety one of its provisions [Art. 6(2)]:

The public concerned shall be informed, either by public notice or individually as appropriate, early in an environmental decision-making procedure, and in an adequate, timely and effective manner, *inter alia*, of:

- (a) the proposed activity and the application on which a decision will be taken;
- (b) the nature of possible decisions or the draft decision;
- (c) the public authority responsible for making the decision;
- (d) the envisaged procedure, including, as and when this information can be provided:
 - (i) the commencement of the procedure;
 - (ii) the opportunities for the public to participate;
 - (iii) the time and venue of any envisaged public hearing;
 - (iv) an indication of the public authority from which relevant information can be obtained and where the relevant information has been deposited for examination by the public;
 - (v) an indication of the relevant public authority or any other official body to which comments or questions can be submitted and of the time schedule for transmittal of comments or questions; and
 - (vi) an indication of what environmental information relevant to the proposed activity is available; and
- (e) the fact that the activity is subject to a national or transboundary environmental impact assessment procedure.

National implementations of these provisions could go even more into details. Here let me take the UK as an example: Arts 13-18 of the Town and Country Planning (Environmental Impact Assessment) (England and Wales) Regulations 1999 provide, *inter alia*, that a developer must make a reasonable number of copies of the environmental statement, including a non-technical summary, available to the public, either free of charge or at a fee

⁷¹ United Nations Economic Commission for Europe, Meeting of the Parties to the Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters, *Decision I/7 on Review of Compliance*, Lucca, 21-23 October 2002, ECE/MP.PP/2/Add.8. <http://www.unece.org/fileadmin/DAM/env/pp/documents/mop1/ece.mp.pp.2.add.8.e.pdf>

“reflecting printing and distribution costs”. A notice should be displayed at the development site for at least 21 days accompanied by a local newspaper advertisement.

4.2. Addendum: collection and dissemination of environmental information

Communication-based tools regulate behaviour by enriching the information available to the targeted audience, thereby enabling them to make more informed choices about their behaviour and, it is hoped, to choose to act in a manner that facilitates the attainment of regulatory objectives. The aim is therefore to bring some kind of indirect social pressure to bear on individual decision-making in the hope that it will lead to behavioural change.⁷²

– Morgan Bronwen and Karen Yeung (2007)

In parallel to providing environmental information on the request of a natural or legal person, and beyond the requirements of EIA, public authorities are obliged to collect and widely disseminate environmental information.⁷³ Such an obligation supplements the “passive” aspect of the right to access environmental information. It is built on the idea that these authorities act as a broker of information to which public has a “right to know” and serves at least double aim. The use of environmental information and its disclosure can cost-effectively drive improvements in environmental results. As Bronwen and Yeung claim, public attention might simply be drawn to particular cases of exemplary (“naming and faming”) or woeful (“naming and shaming”) efforts to achieve compliance with regulatory rules and objectives.⁷⁴ On the one hand, as a result of enhanced transparency, individuals who are informed about environmental hazards in their communities can make more rational decisions about their own protection. On the other hand, such disclosure would motivate industry to take action to prevent them from being viewed as a poor environmental performer.⁷⁵

Let me analyse briefly two examples of such active promotion of environmental information. First, in the United States, the Emergency Planning and Community Right-to-Know Act of 1986⁷⁶ requires companies to report annually the quantity of hazardous chemicals that they have released into the environment or transferred off-site. The United States Environmental Protection Agency then incorporates this information into the Toxic Release Inventory (TRI), which is a nationalised database freely accessible over the Internet,⁷⁷ and subsequently issues an annual report naming those facilities that have released the most toxic substances. Since no company wants to be near the top of the list and thus they come up with their own way of improving the environmental performance, the TRI has been seen as a tremendous success due to its cost-effective substantial reduction of chemical releases.⁷⁸ It could be argued, however, that access to such data could be equally achieved by the means of the freedom of information request, but it is the TRI that had shortcut the bureaucratic information request and made data truly accessible.⁷⁹

Yet the experience of functioning of such inventories shows that data gathered are sometimes difficult to understand any fully exploit, that these data might be misrepresentative without

⁷² Bronwen and Yeung, op. cit., p. 96.

⁷³ Art 5 of the Aarhus Convention.

⁷⁴ Bronwen and Yeung, op. cit., p. 101.

⁷⁵ Herb, Jeanne, Susan Helms and Michael J. Jensen, *Harnessing the 'Power of Information': Environmental Right to Know as a Driver of Sound Environmental Policy*, in Thomas Dietz and Paul C. Stern (eds.), *New Tools for Environmental Protection: Education, Information, and Voluntary Measures*, National Research Council, Washington, 2002, p. 254.

⁷⁶ Emergency Planning and Community Right-to-Know Act of 1986 (EPCRA), 42 U.S.C. § 9601 et seq.

⁷⁷ United States Environmental Protection Agency, *Toxics Release Inventory (TRI) Program*. <http://epa.gov/tri/>

⁷⁸ Hirsch, op. cit., p. 57.

⁷⁹ Herb, Helms, Jensen, op. cit., p. 253.

context (both reasons due to the lack of technical knowledge impeding interpretation) and that chemical volumes are alone poor indicators of human health risks. Individuals are overwhelmed by the amount of this kind of “practical” information. If they are not affected directly by an environmental hazard, they are unlikely to pay attention to data so “remote” from them. From the policy-making viewpoint, many companies switch to use the chemicals that they do not need to report or simply fail to report. Therefore, some authors suggested that in a first place the data should be clear, put into context and cover as many facilities as possible. Second, these data should be distributed effectively, widely available to those with and without computers and people need to know that the information exists. Finally, individuals need both a meaningful reason to track down information and the skills to take advantage of it.⁸⁰

Second, some jurisdictions have in the recent decade introduced a requirement to report on environmental performance in the company’s annual reports.⁸¹ (In other jurisdictions some companies include these data voluntarily.) For example, these reports in Australia have included, *inter alia*, the impacts their activities on the environment, management of environmental risk, usage of resources, exposure to regulation, breaches and how they rectify and prevent future breaches, supply chain policy and the involvement of the board in environmental performance.⁸² (The scope of such reporting might be broadened: in 2012 it was announced that the UK would make publicly listed companies report their greenhouse-gas output, the first country to do so.)⁸³ The Australian experience also shows that not all the reports are meaningful and that mandatory reporting should be coupled with guidance and enforcement by a regulating authority.⁸⁴

4.3. Environmental democracy in the Strasbourg Court: a matter of fundamental rights importance

We have already pointed out that in the past 25 years the Strasbourg Court has made a positive contribution to the construction of an environmental dimension of several rights enshrined in the Convention. ... The Strasbourg case law has contributed to the development of certain ‘environmental obligations’ incumbent upon states parties by virtue of the Convention.⁸⁵

– Francesco Francioni (2010)

In the second section I claimed that public participation in decision-making constitutes a requirement derived from international fundamental rights. Let me here develop this argument further by analysing in a greater detail the relevant case law of the ECtHR.

Cases dealing with environmental issues appear quite often on the Strasbourg Court agenda.⁸⁶ Although the European Convention does not provide an explicit right to a clean and healthy

⁸⁰ Ibid., p. 258.

⁸¹ Cf. Art 5(6) of the Aarhus Convention which stipulates that „Each Party shall encourage operators whose activities have a significant impact on the environment to inform the public regularly of the environmental impact of their activities and products, where appropriate within the framework of voluntary eco-labelling or eco-auditing schemes or by other means.”

⁸² Bubna-Litic, Karen, “Environmental Reporting as a Communications Tool: A Question of Enforcement?,” *Journal of Environmental Law*, Vol. 20, No. 1, 2008, p. 82.

⁸³ Bakewell, Sally, “U.K. to Require Public Companies to Report CO2 Emissions”, Bloomberg, 20 June 2012. <http://www.businessweek.com/news/2012-06-20/u-dot-k-dot-to-require-public-companies-to-report-co2-emissions>

⁸⁴ Bubna-Litic, op. cit., p. 84.

⁸⁵ Francioni, op. cit., p. 49.

⁸⁶ ECtHR, *Environment-related cases in the Court’s case law*, factsheet, Strasbourg, December 2012, http://www.echr.coe.int/NR/rdonlyres/0C818E19-C40B-412E-9856-44126D49BDE6/0/FICHES_Environnement_EN.pdf

environment, the Court's case law has been defining the extent to which the Convention and its Protocols can be relied upon to provide some form of environmental protection and a means of redress (i.e. the "greening" of human rights law).⁸⁷ As the Court recently pointed out in *Kyrtatos v. Greece* (2003),⁸⁸ "neither Article 8 nor any of the other Articles of the Convention are specifically designed to provide general protection of the environment as such", the relevant rights invoked to obtain environmental protection usually include the right to life (Art. 2), the right to fair trial (Art. 6), the freedom of expression (Art. 10), the right to property (Art. 1 of the Additional Protocol No 1) and – most frequently and importantly – the right to protect private and family life, home and correspondence (Art. 8).⁸⁹

Specifically concerning Art. 8, the Court has developed a number of positive obligations⁹⁰ for protecting the interests safeguarded by the right to privacy. From a historical perspective, the first cases dealt with the right to protection of family life and one of the first requirements developed was that of participation.⁹¹ For example, in *W. v. the United Kingdom* (1987),⁹² the Court wanted to determine whether the decision-making process to put a child into care "has been conducted in a manner that, in all the circumstances, is fair and affords due respect to the interests protected by Article 8". In particular,

the relevant considerations to be weighed by a local authority in reaching decisions on children in its care must perforce include the views and interests of the natural parents. The decision-making process must ... be such as to secure that *their views and interests are made known to and duly taken into account* by the local authority and that they are able to *exercise in due time any remedies available to them* ... In the Court's view, what therefore has to be determined is whether, having regard to the particular circumstances of the case and notably the serious nature of the decisions to be taken, *the parents have been involved in the decision-making process, seen as a whole, to a degree sufficient to provide them with the requisite protection of their interests* [§§ 63-64; emphasis added].

This requirement of participation has progressively become a standard in cases related to the placement of children into public care, access rights of parents, the withdrawal of parental responsibility and custody. Ever since, the statement that "the decision-making process leading to measures of interference must be fair and such as to afford due respect for the interests safeguarded to the individual by Article 8"⁹³ spread from family life cases to other

⁸⁷ „It is self-evident that insofar as we are concerned with the environmental dimensions of rights found in avowedly human rights treaties ... then we are necessarily talking about a 'greening' of existing human rights law rather than the addition of new rights to existing treaties". Boyle, Alan, "Human Rights and the Environment: Where Next?," *European Journal of International Law*, Vol. 23, No. 3, October 15, 2012, p. 614.

⁸⁸ ECtHR, *Kyrtatos v. Greece*, Judgement of 22 May 2003, Application no. 41666/98, § 52.

⁸⁹ Stookes, Paul, *A Practical Approach to Environmental Law*, Oxford University Press, 2009, pp. 45-50.

⁹⁰ For the analysis of the concept of positive obligations in the Strasbourg system, cf. e.g. Mowbray, Alastair, *The Development of Positive Obligations Under the European Convention on Human Rights by the European Court of Human Rights*, Hart Publishing, 2004; Akandji-Kombe, J.F., *Positive Obligations under the European Convention on Human Rights. A Guide to the Implementation of the European Convention on Human Rights*, Human Rights Handbooks, Council of Europe, 2007; Bates, Ed, *The Evolution of the European Convention on Human Rights: From Its Inception to the Creation of a Permanent Court of Human Rights*, Oxford University Press, 2010; Xenos, Dimitris, *The Positive Obligations of the State Under the European Convention of Human Rights*, Oxford University Press, 2012.

⁹¹ Brems, Eva, and Laurens Lavrysen, "Procedural Justice in Human Rights Adjudication: The European Court of Human Rights," *Human Rights Quarterly*, Vol. 35, No. 1, 2013, pp. 191-193. This paper also offers a detailed list of cases dealing with each of these issues.

⁹² ECtHR, *W. v. the United Kingdom*, Judgement of 8 July 1987, Application No. 9749/82, § 62.

⁹³ E.g. ECtHR, *McMichael v. the United Kingdom*, Judgement of 24 February 1995, Application No. 16424/90, § 87; ECtHR, *Buckley v. The United Kingdom*, Judgement of 29 September 1996, Application No. 20348/92, § 76.

cases under Art. 8, dealing with issues such as deprivation of legal capacity, data registration, registration of ethnic identity, access to abortion and – notably – environment.⁹⁴

In a number of cases related to environmental issues, the Court has explicitly referred to the need to provide access to information, public consultations and access to justice. Let me use the case of *Taskin et al. v. Turkey* (2004)⁹⁵ to illustrate that. As Francioni observed, “this case is noteworthy for the emphasis the Court places on the procedural duties concerning provision of information and consultation with affected parties as a condition for the fulfilment of the obligations inherent in Article 8”.⁹⁶ First, the Court emphasised the need for informed decision-making, to be achieved by means of “appropriate investigations and studies” that should be subsequently available to the public:

Where a State must determine complex issues of environmental and economic policy, the decision-making process must firstly involve *appropriate investigations and studies* in order to allow them to predict and evaluate in advance the effects of those activities which might damage the environment and infringe individuals’ rights and to enable them to strike a fair balance between the various conflicting interests at stake (see *Hatton and Others* ... § 128). The importance of *public access to the conclusions of such studies and to information which would enable members of the public to assess the danger to which they are exposed* is beyond question (see, *mutatis mutandis*, *Guerra and Others v. Italy*, judgment of 19 February 1998 ... § 60, and *McGinley and Egan v. the United Kingdom*, judgment of 9 June 1998 ... § 97) [§ 119; emphasis added].⁹⁷

Next, the Court emphasised the need for public consultations in decision-making:

It is therefore necessary to consider all the procedural aspects, including the type of policy or decision involved, the extent to which the *views of individuals were taken into account throughout the decision-making process*, and the *procedural safeguards available* (see *Hatton and Others*, cited above, § 104) [§ 118, emphasis added].

Finally, the Court stressed the need for access to justice if the interests safeguarded by Art. 8 were violated:

Lastly, the individuals concerned must also be able to *appeal to the courts* against any decision, act or omission where they consider that their interests or their comments have not been given sufficient weight in the decision-making process (see, *mutatis mutandis*, *Hatton and Others*, cited above, § 127) [§ 119, emphasis added].

In *Giacomelli v. Italy* (2006),⁹⁸ the Court referred explicitly to a positive obligation to conduct an environmental impact assessment:

[The Court] considers that the procedural machinery provided for in domestic law for the protection of individual rights, in particular *the obligation to conduct an environmental-impact assessment* prior to any project with potentially harmful environmental consequences and the possibility for any citizens concerned to participate in the licensing procedure and to submit their own observations to the judicial authorities and, where appropriate, obtain an order for the suspension of a dangerous activity, were deprived of useful effect in the instant case for a very long period [§ 94, emphasis added].

Consistent with the foregoing, the Strasbourg Court reaffirmed, that when it comes to the right to privacy (Art. 8), the three procedural rights – access to information, public participation in decision-making and access to justice – are of vital importance to fundamental

⁹⁴ Brems and Lavrysen, op. cit., pp. 191-193.

⁹⁵ ECtHR, *Taskin and others v. Turkey*, Judgement of 10 November 2004, Application No. 46117/99, § 118.

⁹⁶ Francioni, op. cit., pp. 49-50.

⁹⁷ Some of these positive obligations appeared earlier in: ECtHR, *Hatton and Others v. the United Kingdom*, Judgement of 8 July 2003, Application No. 36022/97.

⁹⁸ ECtHR, *Giacomelli v. Italy*, op. cit.

rights. In result, this case law has an effect of introducing into European human rights, by way of interpretation, the concept of environmental democracy.⁹⁹

4.4. Environmental democracy in the Luxembourg Court: practical application explained

The functioning of environmental democracy has been reviewed by courts at various levels and in various jurisdictions. Since the Aarhus Convention it has been also subject to oversight by the convention's Compliance Committee acting as an advisory body.¹⁰⁰ Such case law offers an invaluable insight into everyday application of environmental democracy.

The ECJ, taken here as an example, dealt with environmental democracy for the first time in *Plaumann* case (1963),¹⁰¹ i.e. long before the environmental procedural rights were formalised under the Aarhus Convention and subsequently implemented into the EU legal order.¹⁰² After *Plaumann*, a number of significant cases followed; they are analysed elsewhere.¹⁰³ Here let me refer only to a few recent cases dealing with the questions of practical application on the Convention's provisions.

The bulk of recent ECJ cases about environmental democracy deal with costs.¹⁰⁴ As Art. 9(4) of the Aarhus Convention establishes, *inter alia*, an obligation of costs protection, in *Commission v Ireland* (2006)¹⁰⁵ the ECJ has sanctioned participation fees as long as they do not create an obstacle to the right to participate in the EIA process.¹⁰⁶ In *Commission v Ireland* (2009),¹⁰⁷ the Court scrutinised the discretion vested in a national court when it comes to the costs of an unsuccessful party:

Although it is common ground that the Irish courts may decline to order an unsuccessful party to pay the costs and can, in addition, order expenditure incurred by the unsuccessful party to be borne by the other party, that is merely a discretionary practice on the part of the courts. That mere

⁹⁹ Francioni, op. cit., pp. 49-50. Francioni refers here to the observation made by Boyle in: Boyle, Alan, "Human Rights or Environmental Rights? A Reassessment", *Fordham Environmental Law Review* (2007) 471, at 497.

¹⁰⁰ United Nations Economic Commission for Europe, *Compliance Committee – Documents*. <http://www.unece.org/env/pp/ccdocuments.html>

¹⁰¹ ECJ, *Plaumann & Co. v Commission*, Judgement of 15 July 1963, Case C-25/62.

¹⁰² The Aarhus Convention has been implemented into the European Union law by the patchwork of legal instruments; the key ones include: Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC, OJ L 41, 14.2.2003, pp. 26–32; Directive 2003/35/EC of the European Parliament and of the Council of 26 May 2003 providing for public participation in respect of the drawing up of certain plans and programmes relating to the environment and amending with regard to public participation and access to justice Council Directives 85/337/EEC and 96/61/EC, OJ L 156, 25.6.2003, pp. 17–25; and Regulation (EC) No 1367/2006 of the European Parliament and of the Council of 6 September 2006 on the application of the provisions of the Aarhus Convention on Access to Information, Public Participation in Decision-making and Access to Justice in Environmental Matters to Community institutions and bodies, OJ L 264, 25.9.2006, pp. 13–19.

¹⁰³ United Nations, Economic and Social Council, Economic Commission for Europe, *Report of the Compliance Committee – Addendum – Findings and recommendations with regard to communication ACCC/C/2008/32 (Part I) concerning compliance by the European Union*, Geneva, 14 April 2011, ECE/MP.PP/C.1/2011/4/Add.1, at 20-31. http://www.unece.org/fileadmin/DAM/env/pp/compliance/CC-32/ece.mp.pp.c.1.2011.4.add.1_as_submitted.pdf. Cf. also Schall, Christian, "Public Interest Litigation Concerning Environmental Matters before Human Rights Courts: A Promising Future Concept?," *Journal of Environmental Law*, Vol. 20, No. 3, 2008, pp. 417–453.

¹⁰⁴ For the analysis of the UK courts practice on fees, cf. ECJ, *Opinion of Advocate General Kokott*, 12 September 2013 in Case C-530/11, *European Commission v the UK*.

¹⁰⁵ ECJ, *Commission v. Ireland*, Judgement of 9 November 2006, Case C-216/05.

¹⁰⁶ Ryall, Áine, "EIA and Public Participation: Determining the Limits of Member State Discretion," *Journal of Environmental Law*, Vol. 19, No. 2, 2007, pp. 247–257.

¹⁰⁷ ECJ, *Commission v. Ireland*, Judgement of 16 July 2009, Case C-427/07.

practice ... cannot, by definition, be certain ... [and] cannot be regarded as valid implementation of the obligations arising from [the EU law] [§ 93].

In *Edwards and Pallikaropoulos v Environment Agency* (2013),¹⁰⁸ the Court elaborated on the concept of “prohibitively expensive” judicial procedures:

The requirement ... that judicial proceedings should not be prohibitively expensive means that the persons covered by those provisions should not be prevented from seeking, or pursuing a claim for, a review by the courts ... by reason of the financial burden that might arise as a result.

... the national court cannot act solely on the basis of that claimant’s financial situation but must also carry out an objective analysis of the amount of the costs. It may also take into account the situation of the parties concerned, whether the claimant has a reasonable prospect of success, the importance of what is at stake for the claimant and for the protection of the environment, the complexity of the relevant law and procedure, the potentially frivolous nature of the claim at its various stages, and the existence of a national legal aid scheme or a costs protection regime [operative part].

Another group of cases deals predominantly with *locus standi*:

- In *Djurgården-Lilla Värtans Miljöskyddsförening v Stockholms kommun genom dess marknämnd* (2009)¹⁰⁹ the ECJ found that members of the public concerned must be able to have access to a review procedure to challenge the decision on development consent, regardless of the role they might have played in the examination of the request (e.g. by taking part in the procedure before that body and by expressing their views). Furthermore, the Court ruled that the right to bring an appeal against a decision on projects cannot be reserved only to environmental protection associations which have at least 2 000 members.
- In *Bund für Umwelt und Naturschutz Deutschland, Landesverband Nordrhein-Westfalen eV v Bezirksregierung Arnsberg* (2011),¹¹⁰ the Court ruled that the EU law precludes legislation which does not permit non-governmental organisations promoting environmental protection to rely before the courts on the ground that that rule protects only the interests of the general public and not the interests of individuals.
- In *Lesoochránárske zoskupenie VLK v Ministerstvo životného prostredia Slovenskej republiky* (2011),¹¹¹ the court stated that “the provisions of Article 9(3) of the Aarhus Convention do not contain any clear and precise obligation capable of directly regulating the legal position of individuals. Since only members of the public who meet the criteria, if any, laid down by national law are entitled to exercise the rights provided for in Article 9(3), that provision is subject, in its implementation or effects, to the adoption of a subsequent measure”. Therefore the said provision “does not have direct effect in European Union law”. Since “those provisions, although drafted in broad terms, are intended to ensure effective environmental protection” it is for the national court “to interpret its national law in a way which, to the fullest extent possible, is consistent with the objectives laid down in Article 9(3)”.

¹⁰⁸ ECJ, *The Queen, on the application of David Edwards and Lilian Pallikaropoulos v Environment Agency and Others*, Judgement of 11 April 2013, Case C-260/11.

¹⁰⁹ ECJ, *Djurgården-Lilla Värtans Miljöskyddsförening v Stockholms kommun genom dess marknämnd*, Judgement of 15 October 2009, Case C-263/08.

¹¹⁰ ECJ, *Bund für Umwelt und Naturschutz Deutschland, Landesverband Nordrhein-Westfalen eV v Bezirksregierung Arnsberg*, Judgement of 12 May 2011, Case C-115/09.

¹¹¹ ECJ, *Lesoochránárske zoskupenie VLK v Ministerstvo životného prostredia Slovenskej republiky*, Judgement of 8 March 2011, Case C-240/09, §§ 45-52.

- In *Flachglas Torgau GmbH v Federal Republic of Germany* (2012)¹¹² the Court ruled that the option given to Member States of not regarding bodies or institutions acting in a legislative capacity as public authorities (Art. 2(2) of the Aarhus Convention) can no longer be exercised where the legislative process in question has ended. Accordingly, in a situation when individuals cannot gain access to environmental information during the legislative process (since the provision of information to citizens is usually adequately ensured in the legislative process), they can do so after the legislative measure has been adopted and therefore information can be obtained for the purposes of challenging the legislative measure subsequent to its adoption.

Recently the Aarhus Convention's Compliance Committee was requested to examine the compliance of the European Union law with the Convention,¹¹³ and in particular with regard to the *locus standi* of environmental associations. Put simply, the jurisprudence of the EU courts shows that such associations are practically barred from bringing cases to these courts. The way in which these courts interpret the requirement of "direct and individual concern" – a prerequisite for *locus standi* in the EU courts – does not comply with the spirit of the Convention, whose broad interpretation should be presumption and not the exception.¹¹⁴

As the preceding sub-sections show, environmental law offers a complex and stringent framework for access to information, public participation in decision-making on specific issues and access to justice in environmental matters. This framework stems from fundamental rights and it benefits from extensive judicial and quasi-judicial interpretation. In the next section I shall demonstrate how this framework can be adapted to the needs of privacy governance.

5. What can the protection of privacy and personal data learn from environmental law?

5.1. Adaptation of environmental democracy to the needs of privacy governance

Even more valuable is the requirement that citizens concerned by new technologies and processing operations are heard and given the necessary facts and data coming from impact assessments.¹¹⁵

– Paul De Hert (2012)

There is undoubtedly a need for the public voice to be heard decision-making, and in particular when privacy is or might be intruded by new technologies.¹¹⁶ Although there is a consensus that public participation is crucial for successful impact assessments and thus should be a core element thereof, the *status quo* of such participation in the process of PIA

¹¹² ECJ, *Flachglas Torgau GmbH v Federal Republic of Germany*, Judgement of 14 February 2012, Case C-204/09.

¹¹³ United Nations, Economic and Social Council, Economic Commission for Europe, *Report of the Compliance Committee – Addendum – Findings and recommendations with regard to communication ACCC/C/2008/32 (Part I) concerning compliance by the European Union*, Geneva, 14 April 2011, ECE/MP.PP/C.1/2011/4/Add.1, at 20-31. http://www.unece.org/fileadmin/DAM/env/pp/compliance/CC-32/ece.mp.pp.c.1.2011.4.add.1_as_submitted.pdf

¹¹⁴ Poncelet, Charles, "Access to Justice in Environmental Matters – Does the European Union Comply with Its Obligations?," *Journal of Environmental Law*, Vol. 24, No. 2, July 2012, pp. 287–309. Krämer, Ludwig, *Access to justice in environmental matters, in particular by NGOs* [manuscript].

¹¹⁵ De Hert, op. cit., p. 75.

¹¹⁶ De Hert, op. cit., pp. 70-72. Furthermore, the European Commission argues for its regulatory impact assessment to include in its scope all fundamental rights foreseen in the EU Charter. Cf. European Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights*, Brussels, 19 October 2010, COM(2010) 573 final, at 1.1.2.

leaves much to be desired. The legislative framework, case law, scholarship and practice of environmental democracy can provide valuable ideas for the protection of privacy in the digital era, and in particular for engaging stakeholders. At least three major lessons can be drawn, subject to necessary adaptations to the reality of the privacy governance.

First, environmental law has conceptualised and developed a comprehensive, three-pillar framework for environmental democracy, in which access to environmental information is a prerequisite for meaningful participation in decision-making on specific activities and in which due account must be given to the results of public consultations. To strengthen these rights, effective access to justice is offered should any of them be violated. As the Aarhus Convention offers minimum standards, the state parties can go beyond and provide a higher level of protection. Furthermore, within the context of Art. 8 of the European Convention, these rights are a matter of fundamental rights importance.

Second, two pillars of environmental democracy, i.e. access to environmental information and participation in environmental decision-making constitute enforceable rights, safeguarded by the third pillar, i.e. effective access to justice. Any limitations to these rights must be interpreted restrictively. The way the parties to the Convention implement its provisions and how these rights are exercised in practice is monitored by the Convention Compliance Committee. It is this rights-based approach and international monitoring that contribute to the efficiency of this framework.

Third, dissemination of environmental information, by means of e.g. release inventories or corporate reporting on environmental performance, enhances transparency and thus allows the individuals to make informed decisions about their own protection as well as forces industry to perform well with regard to the environment.¹¹⁷

From a formal point of view, environmental law offers stringent regulation. The legal provisions are very detailed and deal with issues ranging from the content of the public notice or the environmental report to the time frames for participation. Furthermore, environmental democracy has been extensively interpreted by the courts and other bodies. These institutions, supplemented by the critical perspective of academia, have offered further clarification of already detailed provisions, creating unprecedented knowledge about the practical application of environmental democracy.

These characteristics of environmental democracy make it appealing for its adaptation to the needs of privacy protection. A comprehensive and adequately prescriptive three-pillar framework for the “privacy democracy”, comprising of a right to access information (both “passively” and “actively”), to take part in decision-making in specific situations and to seek remedy if any of these were violated, seems attractive. Environmental law suggests providing not only the individuals but also the general public information about the performance of the entity with regard to the protection of privacy. Environmental law also suggests where the limits of public participation are, i.e. those situations that can have a significant impact on environment. Thus, if we look only at PIA and, assuming that such an adaptation would be achieved by means of hard-law, it might benefit most from establishing an enforceable right to access privacy-related information, to take part in PIA and – finally – to seek remedy,

¹¹⁷ Hirsch already discussed how “public disclosure” could serve as a model for privacy protection by proposing a scheme that would require companies that collect and use personal information to report annually how much of it they released that year. Such a report would include both intentional releases (e.g. transfers of information to affiliates or other third parties) and unintentional ones (e.g. data security breaches). Hirsch, *op. cit.*, pp. 57-58.

should these two be violated. This could be supplemented by an obligation to widely disseminate information on “privacy performance”.

5.2. Possible limitations

Privacy, like the weather, is something everyone talks about. ... In an effort to learn and to legitimate, the ideal PIA involves relevant “stakeholders”. This democratic impulse is admirable, but who decides who is a legitimate stakeholder? – e.g., do those arrested, but not charged or found guilty, have a seat at the table when decisions are made about preserving DNA?¹¹⁸

– Gary T. Marx (2012)

Adapting the framework for environmental democracy to the needs of the protection of privacy would undoubtedly face certain limitations. Below, I analyse some of the most pertinent examples

First and foremost, would the public actually take part in decision-making in privacy matters? What would trigger their interest to participate? This inquiry goes beyond the legal viewpoint on which this paper is based and a number of factors need to be analysed. Yet it shall suffice here to mention that certain differences between “environment” and “privacy” could have decisive impact on the participation of the public.¹¹⁹ One of the concerns is that privacy harms are rather obscured in comparison with environmental ones. Whereas it is possible to observe and measure the direct results of much of environmental pollution, arguments against excessive invasion of privacy often have to be pitched in terms of abstract rights and fears of hypothetical consequences.¹²⁰ Furthermore, while environmental issues “tend to bundle around strip mining and air pollution”,¹²¹ privacy issues are decentralized and pervasive. Another concern is that privacy harms are highly contextual and subjective while those resulting from environmental degradation are rather more objective. Likewise, the appropriate level of privacy protection is only something that can be decided at an individual level, and according to the highly variable instincts about what is, and is not, intrusive or sensitive.¹²² This is linked to the next concern in which it is some form of collective threat to a common good in a given (local) community that would trigger collective response; think of e.g. a nuclear power station being planned in the neighbourhood. Taking all these arguments into account, participation of the public most probably would be produced by big-scale initiatives in which there exists visible and somehow measurable threat to the right to privacy and in which many individuals (and/or their organisations) feel that that right might be threatened. A further argument can be made that the interest to take part in privacy decision-making often would be a function of the role that “privacy culture” plays in a given society.

Second, it might be argued that certain issues are already covered. With regard to the first pillar of environmental democracy (access to information), both the freedom of expression, in particular its passive aspect (i.e. right to receive information), and the laws on freedom of information can ensure access to information. However, they lack greater specificity and particular focus as well as constitute a complicated procedure to follow. As the Strasbourg Court observed, Art. 10 ECHR “guarantees not only the freedom of the press to inform the public but also the right of the public to be properly informed”¹²³ yet it does not impose on

¹¹⁸ Marx, Gary T., “Privacy Is Not Quite Like the Weather” in Wright and De Hert, op. cit., pp. v-xiv.

¹¹⁹ I thank Colin J. Bennett for bringing this matter to my attention.

¹²⁰ Bennett, Colin, *The Privacy Advocates. Resisting the Spread of Surveillance*, MIT Press, 2008, p. 213.

¹²¹ Valerie Steeves quoted in Bennett, Colin, *The Privacy Advocates...*, op. cit., pp. 210-214.

¹²² Bennett, op. cit., pp. 210-214.

¹²³ ECtHR, *Sunday Times v the United Kingdom*, Judgement of 26 April 1979, Application No. 6538/74, § 66.

public authorities “positive obligations to collect and disseminate information of its own motion”.¹²⁴

Furthermore, in the current EU data protection framework, the data subject (i.e. an individual) already has a right to be informed about her personal data being processed,¹²⁵ *de facto* supplemented by privacy policies. Some initiatives – voluntary ones or not – have been already undertaken, e.g. data breach notifications,¹²⁶ transparency reports (e.g. Google,¹²⁷ Microsoft¹²⁸ and – recently – Vodafone)¹²⁹ or publication of PIA reports (or summaries thereof).¹³⁰ However, vast majority of these initiatives focus on one particular aspect of privacy and do not give a broader picture how privacy is addressed in a given organisation.

With regard to the second pillar, i.e. participation in decision-making, in the EU, Art. 33(4) of the proposed General Data Protection Regulation¹³¹ requires a data controller, while performing a DPIA, to “seek the views of data subjects or their representatives on the intended processing”. If entered into force and in the current shape it could be argued that it would create a right to take part in such an assessment. This would be strengthened by a number of remedies and sanctions.¹³² However, this particular aspect of participation would be limited by the scope of DPIA foreseen in this proposed Regulation, thus omitting other types of privacy.

It might also be argued that a three-pillar framework for “privacy democracy”, if mandatory, would just create more “red tape” and would not receive support neither from policy-makers nor from the private sector. However, this negative effect could be minimized by the benefits a project’s sponsor could get (cf. *supra*, section 2), by a careful design as well as by minimal cost and disruption of such a framework, among others.

¹²⁴ ECtHR, *Guerra et al. v Italy*, Judgement of 19 February 1998, Application No. 14967/89, § 53.

¹²⁵ Cf. Arts 10-11 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, pp. 31-50.

¹²⁶ Cf. 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 (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, pp. 37-47.

¹²⁷ Google, *Transparency Report*. <http://www.google.com/transparencyreport/userdatarequests/>

¹²⁸ Microsoft, 2012 *Law Enforcement Requests Report*. <http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/>

¹²⁹ “Vodafone is to take a stand on privacy by asking British ministers, and the governments of each of the 25 countries in which it operates, for the right to disclose the number of demands it receives for wiretapping and customer data.” Garside, Juliette, *Vodafone takes a stand on privacy with plan to disclose wiretapping demands*, The Guardian, 15 January 2014. <http://www.theguardian.com/business/2014/jan/15/vodafone-aims-to-disclose-wiretap-demands>

¹³⁰ The RFID Recommendation (op. cit.) repeats certain requirements of the Directive 95/46/EC (op. cit.), i.e. the information about the controller and about the purpose of processing (Arts 10-11), but it suggests further to include additionally the categories of personal data involved, the summary of privacy impact assessment carried out with regard to the RFID application in question and the information about the likely privacy risks.

¹³¹ European Commission, *Proposal...*, op. cit., fn. 53.

¹³² In particular, Art 73 introduces the right to lodge a complaint with a supervisory authority if the data subject “consider[s] that the processing of personal data relating to [her] does not comply with [the Regulation]”. Art 75 provides for a right to a judicial remedy against a controller or processor “if [data subjects] consider that their rights under [the] Regulation have been infringed as a result of the processing of their personal data in non-compliance with [the] Regulation”. By virtue of Art 77 “any person who has suffered damage as a result of ... an action incompatible with [the] Regulation shall have the right to receive compensation”. Finally, a supervisory authority would be able impose a fine “to anyone who, intentionally or negligently ... does not carry out a data protection impact assessment” [Art 79(6)(i)]. However, it remains an open question if the remedies foreseen in the proposed General Data Protection Regulation are structurally similar to those in environmental law.

5.3. Suggestions for further research

Apart from investigating the above-mentioned possible limitations, a few suggestions for further research can be made. First, as the concept of “environmental information” is well defined in broad terms in the environmental law,¹³³ the scope of “privacy information” could be defined too. Second, the scope of “privacy performance reporting” needs to be demarcated. Both public and private sector organisations certainly need to report issues such as their privacy policies and their amendments, PIA reports (or meaningful summaries thereof), statistics on data transfers to other data controllers, and in particular to other jurisdictions, data breaches as well as law enforcement requests. However, individuals may need more information on how privacy issues are managed within an organisation. Third, it should be analysed what is the stance of the Strasbourg Court – and other constitutional or international human rights courts – on the three positive obligations – access to information, participation in decision-making and access to justice – outside the scope of environmental protection. Fourth, particular means of introduction of each of these ideas should be analysed, e.g. soft-law or hard-law, whether this framework should apply to both public and private sector, what should be its territorial scope (international, regional), and how to minimize negative impact thereof, in particular the “red tape”. Fifth, a body to monitor compliance should be created or designated as well as whether – on a national level – it should be a data protection authority.

6. Bibliography

- Akandji-Kombe, J.F., *Positive Obligations under the European Convention on Human Rights. A Guide to the Implementation of the European Convention on Human Rights*, Human Rights Handbooks, Council of Europe, 2007.
- Bakewell, Sally, “U.K. to Require Public Companies to Report CO2 Emissions”, *Businessweek*, Bloomberg, 20 June 2012. <http://www.businessweek.com/news/2012-06-20/u-dot-k-dot-to-require-public-companies-to-report-co2-emissions>
- Bates, Ed, *The Evolution of the European Convention on Human Rights: From Its Inception to the Creation of a Permanent Court of Human Rights*, Oxford University Press, 2010.
- Bayley, Robin, and Colin Bennett, “Privacy Impact Assessments in Canada,” in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer Netherlands, 2012.
- Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate Publishing, 2003.
- Bennett, Colin, *The Privacy Advocates. Resisting the Spread of Surveillance*, MIT Press, 2008.
- Blowfield, Michael, and Alan Murray, *Corporate Responsibility*, Oxford University Press, 2011.
- Bohman, James F., and William Rehg, *Deliberative Democracy: Essays on Reason and Politics*, Cambridge 1997.
- Boyle, Alan, “Human Rights and the Environment: Where Next?,” *European Journal of International Law*, Vol. 23, No. 3, October 15, 2012.
- Boyle, Alan, “Human Rights or Environmental Rights? A Reassessment”, *Fordham Environmental Law Review*, 2007.
- Brems, Eva, and Laurens Lavrysen, “Procedural Justice in Human Rights Adjudication: The European Court of Human Rights,” *Human Rights Quarterly*, Vol. 35, No. 1, 2013.

¹³³ Cf. footnote 70.

- Bronwen, Morgan, and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press, 2007.
- Bubna-Litic, Karen, "Environmental Reporting as a Communications Tool: A Question of Enforcement?", *Journal of Environmental Law*, Vol. 20, No. 1, 2008.
- Clarke, Roger, "An Evaluation of Privacy Impact Assessment Guidance Documents", *International Data Privacy Law*, Vol. 1, No. 2, 2011.
- Clarke, Roger, „Privacy Impact Assessment: Its Origins and Development”, *Computer Law and Security Review*, Vol. 25, No. 2, 2009. <http://www.rogerclarke.com/DV/PIAHist-08.html>
- Creighton, James L., *The Public Participation Handbook: Making Better Decisions Through Citizen Involvement*, Wiley, 2005.
- European Commission, *Impact Assessment Guidelines*, SEC(2009) 92, Brussels, 15.01.2009.
- European Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights*, COM(2010) 573 final, Brussels, 19.11.2010.
- European Commission, *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) 11 final, Brussels, 25.01.2012.
- European Commission, *EU Regulatory Fitness*, COM(2012) 746 final, Brussels, 12.12. 2012.
- De Hert, Paul, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments," in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer Netherlands, 2012.
- De Hert, Paul, Dariusz Kloza and David Wright, *Recommendations for a privacy impact assessment framework for the European Union*, Deliverable D3 of the PIAF project, Brussels, 2012. http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- della Porta, Donatella, *Can democracy be saved? Representation, Participation and Deliberation*, paper presented at conference *Democratic Representation in Crisis: what kinds of theories for what kinds of research, and to what ends?*, Florence, 9-10 April 2013.
- Department of Trade and Industry, *Nanotechnology offers potential to bring jobs, investment and prosperity – Lord Sainsbury*, London, 2004. <http://www.voyle.net/Nano%20Debate/Debate2004-0017.htm>
- Dietz, Thomas, and Paul C. Stern, "Introduction," in Thomas Dietz and Paul C. Stern, *Public Participation in Environmental Assessment and Decision Making*, National Academy of Sciences, 2008.
- Dietz, Thomas, and Paul C. Stern, "The Promise and Perils of Participation," in Thomas Dietz and Paul C. Stern, *Public Participation in Environmental Assessment and Decision Making*, National Research Council, 2008.
- Douglas-Scott, Sionaidh, "Environmental Rights: Taking the Environment Seriously", in Gearty, C. A. and A. Tomkins, *Understanding Human Rights*, Continuum International Publishing Group, 1996.
- ECtHR, *Environment-related cases in the Court's case law*, Strasbourg, December 2012, http://www.echr.coe.int/NR/rdonlyres/0C818E19-C40B-412E-9856-44126D49BDE6/0/FICHES_Environnement_EN.pdf
- European University Institute, *Citizens respond to crisis by reshaping democracy*, press release, Florence, 18 April 2013. <http://www.eui.eu/News/2013/04-18-Citizensrespondtocrisisbyreshapingdemocracy.aspx>
- Francioni, Francesco, "International Human Rights in an Environmental Horizon," *European Journal of International Law*, Vol. 21, No. 1, 2010.

- Garside, Juliette, *Vodafone takes a stand on privacy with plan to disclose wiretapping demands*, The Guardian, 15 January 2014. <http://www.theguardian.com/business/2014/jan/15/vodafone-aims-to-disclose-wiretap-demands>
- Gleick, James, "Big Brother Is Us", *New York Times*, 29 September 1996. <http://www.nytimes.com/1996/09/29/magazine/big-brother-is-us.html>
- Gutmann, Amy, and Dennis Thompson, *Why Deliberative Democracy?*, Princeton, 2004.
- Gutwirth, Serge, Michael Friedewald et al., *Legal, social, economic and ethical conceptualisations of privacy and data protection*, Deliverable D1 of the PRESCIENT project, Karlsruhe, March 2011. <http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT-D1---final.pdf>
- Hart, David, "Aarhus for real beginners", *UK Human Rights Blog*. <http://ukhumanrightsblog.com/n/2013/10/12/aarhus-for-real-beginners>
- Herb, Jeanne, Susan Helms and Michael J. Jensen, *Harnessing the 'Power of Information': Environmental Right to Know as a Driver of Sound Environmental Policy*, in Thomas Dietz and Paul C. Stern (eds.), *New Tools for Environmental Protection: Education, Information, and Voluntary Measures*, National Research Council, Washington, 2002.
- Hildebrandt, Mireille, "Legal and Technological Normativity: More (and Less) than Twin Sisters," *Techné*, Vol. 12, No. 3, 2008. http://works.bepress.com/mireille_hildebrandt/13
- Hirsch, Dennis, "Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law", *Georgia Law Review*, Vol. 41, No. 1, 2006.
- Hosein, Gus, and Simon Davies, *Empirical research of contextual factors affecting the introduction of privacy impact assessment frameworks in the Member States of the European Union*, Deliverable D2 of the PIAF project, August 2012, http://www.piafproject.eu/ref/PIAF_deliverable_d2_final.pdf
- Human Rights Committee, *General Comment No. 25: The Right to Participate in Public Affairs, Voting Rights and the Right of Equal Access to Public Service*, 12 July 1996, CCPR/C/21/Rev.1/Add.7
- International Finance Corporation, *Guide to Human Rights Impact Assessment and Management*, Washington, 2010. http://www.guidetohriam.org/app/images/secure/GuidetoHRIAM_v13_LR.pdf
- International Finance Corporation, *Introduction to Health Impact Assessment*, Washington, 2009, http://www1.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/ifc+sustainability/publications/publications_handbook_healthimpactassessment_wci_1319578475704
- Jayawickrama, Nihil, *The Judicial Application of Human Rights Law: National, Regional and International Jurisprudence*, Cambridge University Press, 2002.
- Kloza, Dariusz, Anna Mościbroda and Gertjan Boulet, "Improving Co-operation Between Data Protection Authorities: First Lessons from Competition Law," *Jusletter IT. Die Zeitschrift Für IT Und Recht*, 2013. <http://jusletter-it.weblaw.ch/issues/2013/20-Februar-2013/2128.html>
- Krämer, Ludwig, *Access to justice in environmental matters, in particular by NGOs*, manuscript.
- Marx, Gary T., "Privacy Is Not Quite Like the Weather", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer Netherlands, 2012.
- Microsoft, *2012 Law Enforcement Requests Report*. <http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency>
- Mowbray, Alastair, *The Development of Positive Obligations Under the European Convention on Human Rights by the European Court of Human Rights*, Hart Publishing, 2004.
- Nehf, James, "Recognizing the Societal Value in Information Privacy", *Washington Law Review*, Vol. 78, 2003.

- Noble, Bram F., *Introduction to Environmental Impact Assessment: A Guide to Principles and Practice*, 2nd ed., Oxford University Press, 2009.
- Organisation for Economic Cooperation and Development, *Stakeholder Involvement Techniques*, Paris, 2004. <http://www.oecd-nea.org/rwm/reports/2004/nea5418-stakeholder.pdf>
- Owens, Phil, *Sediment Management at the River Basin Scale*, Elsevier Science, 2007.
- Poncelet, Charles, "Access to Justice in Environmental Matters – Does the European Union Comply with Its Obligations?," *Journal of Environmental Law*, Vol. 24, No. 2, July 2012.
- Popović, Neil A.F., „The Right To Participate In Decisions That Affect The Environment”, *Pace Environmental Law Review*, Vol. 10, 1993.
- Privacy and Data Protection Impact Assessment Framework for RFID Applications*, Brussels, 12 January 2011. http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf
- Purtova, Nadezhda, *Property Rights in Personal Data: A European Perspective*, Kluwer Law International, 2011.
- Razzaque, Jona, "Information, public participation and access to justice in environmental matters", in Alam, S., J. Bhuyian, T. Chowdhury and E. Techera (eds.), *Routledge Handbook of International Environmental Law*, Routledge, 2012.
- Ryall, Áine, "EIA and Public Participation: Determining the Limits of Member State Discretion," *Journal of Environmental Law*, Vol. 19, No. 2, 2007.
- Sama, Linda M., Stephanie A. Welcomer and Virginia V. Gerde, "Who Speaks for the Trees? Invoking an Ethic of Care to Give Voice to the Silent Stakeholder," in Sanjay Sharna and Mark Starik, *Stakeholders, The Environment And Society*, Edward Elgar Publishing, 2004.
- Schall, Christian, "Public Interest Litigation Concerning Environmental Matters before Human Rights Courts: A Promising Future Concept?," *Journal of Environmental Law*, Vol. 20, No. 3, 2008.
- Stoddart, Jennifer, *Auditing privacy impact assessments: the Canadian experience*, in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer Netherlands, 2012.
- Stone, Christopher D., „Should Trees Have Standing – Toward Legal Rights for Natural Objects”, *South California Law Review*, Vol. 45, 1972.
- Stone, Christopher, *Should Trees Have Standing? Law, Morality, and the Environment*, Oxford University Press, 2010.
- Stookes, Paul, *A Practical Approach to Environmental Law*, Oxford University Press, 2009.
- Tanasescu, Irina, *The European Commission and interest groups. Towards a deliberative interpretation of stakeholder involvement in EU policy-making*, Brussels, 2007.
- Taschner, Stefan, and Matthias Fiedler, *Stakeholder Involvement Handbook*, Deliverable D2.1 of the AENEAS project, 21 April 2009. http://www.aeneas-project.eu/docs/AENEAS_StakeholderInvolvementHandbook.pdf
- United Nations Economic Commission for Europe, *Compliance Committee – Documents*. <http://www.unece.org/env/pp/ccdocuments.html>
- United Nations, Economic and Social Council, Economic Commission for Europe, *Report of the Compliance Committee – Addendum – Findings and recommendations with regard to communication ACCC/C/2008/32 (Part I) concerning compliance by the European Union*, Geneva, 14 April 2011, ECE/MP.PP/C.1/2011/4/Add.1, at 20-31. http://www.unece.org/fileadmin/DAM/env/pp/compliance/CC-32/ece.mp.pp.c.1.2011.4.add.1_as_submitted.pdf
- United Nations, Economic and Social Council, Economic Commission for Europe, *Report of the Compliance Committee – Addendum – Findings and recommendations with regard to*

communication ACCC/C/2008/32 (Part I) concerning compliance by the European Union, Geneva, 14 April 2011, ECE/MP.PP/C.1/2011/4/Add.1, at 20-31.
http://www.unece.org/fileadmin/DAM/env/pp/compliance/CC-32/ece.mp.pp.c.1.2011.4.add.1_as_submitted.pdf

United States Environmental Protection Agency, *Toxics Release Inventory (TRI) Program*.
<http://epa.gov/tri/>

Wilton, Robin, *What's happened to PETs?*, Future Identity, Westbury, 27 September 2009.
<http://ftc.gov/os/comments/privacyroundtable/544506-00076.pdf>

Wright, David, and Emilio Mordini, "Privacy and Ethical Impact Assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer Netherlands, 2012.

Wright, David, "The State of the Art in Privacy Impact Assessment," *Computer Law & Security Review*, Vol. 28, No. 1, 2012.

Wright, David, Kush Wadhwa, Paul De Hert and Dariusz Kloza (eds.), *PIAF: A Privacy Impact Assessment Framework for data protection and privacy rights*. Deliverable D1 of the PIAF project, 21 September 2011. http://www.piafproject.eu/ref/PIAF_D1_21_Sept2011Revlogo.pdf

Wright, David, Raphael Gellert, Serge Gutwirth and Michael Friedewald, "Minimizing Technology Ricks with PIAs, Precaution, and Participation," *IEEE Technology and Society Magazine*, Vol. 30, No. 4, 2011.

Xenos, Dimitris, *The Positive Obligations of the State Under the European Convention of Human Rights*, Oxford University Press, 2012.

PERSONAL DATA PROTECTION AND ACCESS TO PUBLIC INFORMATION: FUNDAMENTAL RIGHTS FOR THE CONSOLIDATION OF DEMOCRACY

Laura Nahabetián Brunet

MP Consultant – Deputy Chamber
SN de las Leyes, Av. Montevideo – Uruguay
lnahabetian@gmail.com

Keywords: *Data protection, public information, fundamental rights, interpretive standard, primacy, conflicts, principles*

Abstract: *The rights to personal data protection and access to public information are fundamental rights. These rights are central to today's representative democracies because they form the basis on which citizens can efficaciously control and influence the decisions made in their name and based on the mandate that the public has given its representatives. Citizens can exercise their freedom effectively to the extent that they can determine who can manage their personal information and under what conditions. To the extent that the right to information and the right to privacy can be seen as complementary rights which at some point can collide, it is necessary to evaluate whether it is relevant that one right outweighs the other right, and which one should yield to the other.*

1. Introduction

The ideologization of the situations that arise daily in society needs to come to an end. The public is calling for forceful measures to be taken to help stabilize a system whose institutionalization has experienced difficulties and is still in the process of consolidation. “It is no longer a matter of ideological debate to show that democracy is a necessary condition for development. Here we are referring to democracy not only as a political system, but also as a system of relations with the citizens that extends beyond the institutional.”¹

“Political stability can only be sustained when democratic institutions are willing to be held accountable to their citizens, when civil society organizations and the social media are allowed to play a greater role, and when women, the poor, the minorities, and the indigenous populations are given greater participation in the process. The strength, efficacy, and autonomy of the political institutions will be crucial when the political system is hit by the recurring crises of governability that will inevitably come.”²

Today, societies are aware that it is not enough for a democracy to ensure the permanent election of representatives, and that it is not enough to merely appeal to the elected representative to abide by ethical standards in their behavior. When faced with corruption, comptrollers must employ

¹ Carrillo, Fernando.- “El déficit de democratización en América Latina”, en Democracia en déficit: Gobernabilidad y Desarrollo en América Latina. BID. Washington (2001).

² Lowenthal, Abraham.- “Latin America at the Century's Turn”, en Journal of Democracy N° 11 Volumen 2. The Johns Hopkins University Press. Baltimore (2000).

procedures and enforce regulations that reduce and even aim to eliminate the temptations of politicians to be unethical.

2. Governability

Camou proposes a broad, multidimensional, relational concept of governability, which he describes as “a state of dynamic equilibrium between the level of social demands and the ability of the government to response.”³ This enables the system to overcome the traditional dichotomy of governability – ungovernability. He suggests that political culture consists of three areas: the norms and institutions of political action; the role of the State; and the role of its public policies, all of which are in a dynamic, ongoing relationship. Governability in its most explicit form includes the following elements: legitimacy, efficacy, efficiency, and stability; where legitimacy refers to a quality; efficacy and efficiency refer to qualifying properties; and stability refers to the state of governability.

“Governability is conceived of as a property of political systems defined by their ability to achieve stated objectives at the lowest cost possible.”⁴

A social system is said to be governable when it is structured from a social and political point of view such that the strategic actors establish interactive relationships that enable them to make joint decisions and resolve conflicts in accordance with a regulatory system and processes, both formal and informal, within a framework which verifies compliance with various levels of expectation and the strategies.

Governability can be said to be democratic to the extent to which the political decisions that are adopted are done so according to established procedures and regulations that are recognized as being democratic in nature. This also applies to situations requiring conflict resolution.

“A democratic system is a system in which the legitimacy of a government stems not just from its ability to hold elections, but also from its ability to sustain a consensus among the citizens that it is indeed legitimate.”⁵

It is essential that the two concepts of democracy and governability are understood as being indissoluble. It is valid to claim that governability is possible without democracy, but it is also valid to claim the possibility of democracy with little or no governability.

It is a fundamental truth that growth is impossible without governability and, likewise, that human development is impossible without governability. Thus, if development is understood as human development, democracy is an inseparable element of the strategy that must be carried out completely independent of the baseline conditions. “In human development theory, freedom is not only the evaluative criterion of institutions, but also the instrumental means for their improvement, which depends on free human agency. Hence, freedom is not only the main goal of development, but is also one of its principal means of attaining development. There is a significant empirical relationship among the various types of freedom: political freedoms (in the form of the freedom of expression and free elections) promote economic security; social opportunities (in the form of educational and health services) facilitate economic participation; economic services (in the form of opportunities to participate in trade and production) can help create personal wealth, along with public resources to finance social services.”⁶

³ *Camou, Antonio.-* Gobernabilidad y Democracia. Cuadernos de Divulgación de la Cultura Democrática N° 6. IFE. México DF (2001).

⁴ *Camou, Antonio.-* Los desafíos de la gobernabilidad: estudio premilitar. Editorial Plaza y Valdés. México DF (2001).

⁵ *Bobbio, Norberto, y otros.-* Diccionario de Política. Siglo XXI Editores. México DF (1988).

⁶ *Sen, Amartya.-* El desarrollo como libertad. Editorial Planeta. Barcelona (1999).

There is also a normative synchronization that strengthens the rights and obligations of the citizens, encouraging their participation in the development process and ensuring accessibility. “The legal system confers and guarantees legal rights. These rights are defined through the political process and protect economic interests. The formal legal system of a sovereign body plays a major role with regard to economics, as it establishes and enforces the basic rules that govern economic exchange. These include not only economic rights, but also the basic political rights that are a prerequisite for exercising those economic rights. However, other informal legal systems also play a significant role in creating and ensuring rights. Formal legal rights do not come pre-defined in the abstract, but rather are the result of the political process and political actors.

The political system is defined by the behavior of interest groups competing for special rights (economic advantages) that fall within the established regulations of the political institutions. Political decisions, whether they are concerned with design or implementation, are transformed into policies and actions by the administrative system by means of a hierarchy of agents acting in the name of their principals (the citizens, politicians, and policy makers).”⁷

It is essential to increase awareness of the critical role that political freedoms play in the area of human development, and, hence, as key determinants of democratic governability. Political freedoms and democratic governability form an inextricable circle that is conceptually, theoretically, and politically inseparable.

“In this way, political freedoms, in a broad sense, which includes human rights, are the constitutive components of development, as well as the instrumental means of carrying out development. Political freedoms express the opportunities that individuals have to decide who will govern and what principles they will govern by. They provide them with the possibility of monitoring and criticizing the authorities, the freedom of political expression, the freedom of the press, the freedom to choose among various political parties, and so on. Political freedoms include the political rights that form an integral part of a democracy, in the broad sense of the word (which covers the possibility of political dialogue, dissent, and criticism), as well as the right to vote and to participate in electing the Legislative Power and the Executive Power.”⁸

2.1. Fundamental rights

To establish human rights as universal fundamental rights is of momentous importance, not only in order to extend them to all human beings without distinction, but also to confirm them as inalienable rights.

It is likewise important to affirm that people are the basic referent of fundamental rights. Thus, the State is obligated not only to respect them, but also to guarantee these rights to its citizens. However, a problematic issue arises when different rights appear to be in conflict and there seems to be no reasonable and just way to apply them. Hence, the goal must be, from the outset, to ensure that all fundamental rights and the duties they entail are harmoniously interrelated, even correlated.

As Ferrajoli puts it, “If these rights ‘are normative’ for ‘everyone’ (all the members of a particular class of subjects), they are not transferable or negotiable, but rather assume the status of, if you will, inalterable, non-contingent privileges of the members and possess such wide-ranging implications that the powers that be, both public and private, must honor them.”⁹

⁷ Dethier, Jean.- Governance and Economic Performance: A Survey. Discussion Papers on Development Policy. Center for Development Reserch. Bonn (1999).

⁸ Idem 6.

⁹ Ferrajoli, Luigi.- Derecho y razón. Editorial Trotta. Madrid (2005).

We are dealing with rights that are not new. They date back hundreds of years, but their effective recognition has come relatively recently and is inextricably linked with democracy and the Rule of Law.

Dworkin suggests that “...individual rights are political triumphs held by individuals. Individuals have rights when, for some reason, a collective goal is not sufficient justification to deny them what they, as individuals, desire to have or do, or when a loss or injury to a person is not sufficiently justified.”¹⁰

Reaffirming this, Alexy states that “the meaning of fundamental rights consists in not allowing decisions about certain individual prerogatives to be made by the parliamentary majority, that is, by delineating the field of decision ...” He concludes brilliantly, “not even by unanimity can a nation decide (or consent to the decision) that an innocent human being should die or be deprived of his liberty, that a human should think or write, or not think or not write, in a certain way, that he/she should not meet or associate with another person, that he/she should marry or not marry with a certain person or stay linked to certain person, that he/she should have or not have children, that he/she does or doesn’t do a certain type of work, and so on. Ensuring these basic rights is an indispensable condition for peaceful coexistence.”¹¹

3. Personal data protection and access to public information

It is important to regard the rights to the personal data protection and access to public information as fundamental rights.

These rights are central to today’s representative democracies because they form the basis on which citizens can efficaciously control and influence the decisions made in their name and based on the mandate that the public has given its representatives. Citizens can exercise their freedom effectively to the extent that they can determine who can manage their personal information and under what conditions.

Countries, such as the Latin American countries, where these rights are currently being drawn up, must advance in an efficient manner toward the implementation of these rights. They must avoid merely making declarations of good intentions, passing unenforceable laws, and making insubstantial decisions that do little to advance the consolidation of democracy in ways that address the undemocratic practices that still exist.

4. The weighting of rights in conflict

4.1. Statutory interpretation

It is essential to consider the interpretive standards that have been established for the statutes associated with human rights, some of which are quite precise in nature.

Three central principles are included here: the principle of *pro homine*, the principle of *pro victima*, and the principle of *pro libertatis*.

Using this as a starting point, it is possible to assert the existence of a series of important bases for interpreting the various statutory provisions of legal acts, notwithstanding the fact that these three principles do not preclude the enforcement of the system of human rights and the corresponding interpretation of the jurists for the purposes of reconciling the rights in accordance with the ultimate goal of permitting the coexistence of the various legal values at stake.

¹⁰ *Dworkin, Ronald.- Los derechos en serio.* Editorial Ariel. Barcelona (1993).

¹¹ *Idem* 10.

4.1.1. The guideline of statute preference

For cases in which there are varying statutes, it is necessary to choose the statute that is the most favorable to the fundamental right at stake, regardless of any prevailing hierarchy.

Applying the principles does not entail modifying the system of human rights. The jurists are responsible for interpreting and reconciling the statutes and the rights. They must balance the values, make them compatible, and facilitate the coexistence of the various rights, all while considering the needs of the common good.

4.1.2. The guideline of preference

For cases in which there are various possible interpretations of a statute, it is necessary to choose the interpretation that best protects human beings.

The principle to be applied here is the principle of *pro libertatis*, which means that the statutory provision must be interpreted in the manner that is the most beneficial to the freedom in question.

The principle of *pro homine* must also be applied to the extent that the Inter-American Court of Human Rights stipulates, which means, on the one hand, that the interpretation must consider human rights, and, on the other hand, that the limitations must be interpreted in a strict sense.

“All the human rights statutes in our legal system must be interpreted in accordance with the respective conventional statutory sources, which are both international and domestic. These rights have been incorporated into the body of law by mandate of the constituent members, establishing limits to sovereignty, that is, limits to the instituted or derived constituent powers and to all the state entities and authorities.”¹²

Human rights always have expansive interpretive power. As Fernandez Segado says, the law should always be interpreted in the broadest sense possible, based on the need to choose the interpretation that will maximize the implications of the law. Exceptions must be interpreted in an absolutely strict sense, and interpretations must be considered invalid if they are of an analogous nature or *contrario sensu* to a statute that establishes an exception to a statutory provision of human rights.

4.2. Primacy or conflict of rights?

To the extent that the right to information and the right to privacy can be seen as complementary rights which at some point can collide, it is necessary to evaluate whether it is relevant that one right outweighs the other right, and which one should yield to the other.

“According to most legal jurists (Alexy, Dworkin), when a collision between fundamental rights is alluded to, one is not implying a true contradiction of legal rules (statutory contradiction), but rather tensions between the legal principles which the rights are endowed with.

This point is of paramount importance because it proposes that the role of a judge is not to merely apply binding, preconceived rules of law, but rather for the judge to perform the role of an interpreter and an integrator of incomplete rights, which consist of more than mere statutes. This is the premise of Dworkin, who quite rightly, by exchanging rules for principles, substitutes mandatory application of statutes with discretionary interpretation and application.

This deals with the creative work of the law which is performed by judges. “Judicial work consists not only in the interpretation of texts, regardless of the procedures involved, nor only in the enforcement of statutes, which is often the role of judges in other types of cases: it includes

¹² Nogueira, Humberto.- Dogmática de los derechos esenciales. <http://www.bibliojuridica.org/libros/3/1094/16.pdf>

valuation, weighting, and balancing reasons, which spotlights the sovereign powers of judicial authority.

Some authors have coined the notion of essential content as those elements that determine the meaning, scope, and conditions of the exercise of fundamental rights. The role of essential content is to prevent excessive caution from being used with respect to the constitutional and legal restrictions or limitations of fundamental rights, because doing so would undermine and empty the fundamental right of content. Thus, the idea behind this notion is that fundamental rights have core content that is inaccessible to legal limitations, which does not imply, in any case, that there are indiscriminate limitations outside the core content.”¹³

It is necessary to look at the weighting of rights to fully develop this point.

The proponents of the balancing test “attempt to weigh the rights in play. The starting point for this is to consider all the rights and goods as being equal and equivalent to each other, which imposes examination and weighting on a case-by-case basis. In general, the proponents of this view do not provide criteria to carry out such a weighting.”¹⁴

The weighting involves application of the principles, which strictly speaking means that these statutes have the profile of mandated optimization, which in the words of Alexy means “that the statute is executed to the fullest extent possible within the existing legal and real possibilities.”¹⁵

“The character of the principle implies the maxim of proportionality:¹⁶ this means that the character of the principle is inferred from the maxim of proportionality, with its three partial maxims of suitability, need (postulated from the most benign means), and proportionality in a strict sense (postulated from the weighting). In a rather obscure formulation, the Federal Constitutional Court has found that the maxim of proportionality “basically arises from the very essence of fundamental rights.” It will be shown below that this is indeed true in the strict sense when the basic statutes reflect the character of the principle.

The principles are mandates of optimization with respect to the legal and factual possibilities. The maxim of proportionality in a strict sense, the mandate of weighting, follows from the relativization of the legal possibilities. If a statute of a fundamental right with the character of a principle clashes with an opposing principle, then the legal possibility of realizing the statute of a fundamental right depends on the opposing principle. In order to overcome the contradiction and reach a decision, a weighting is necessary. Just as the enforcement of valid principles, when they are applicable, is in order, a weighting is called for in the case of opposing principles. This means that the maxim of proportionality in a strict sense is inferred from the character of the principle of the statutes of fundamental rights. From the maxim of proportionality in a strict sense, it follows that the principles are mandates of optimization with regard to the legal possibilities. In contrast, the maxims of need and suitability follow the character of the principles as mandates of optimization with regard to the factual possibilities.

To show how the maxim of need is inferred from the nature of the principle, the simplest scope of the determination of need will be considered here. The fact that the maxim of need presents greater

¹³ *Bauzá, Marcelo.* - “Criterios para armonizar la protección de datos personales y el acceso a la información pública”, en *Anuario de Derecho Informático* N° X. Fundación de Cultura Universitaria. Montevideo (2010).

¹⁴ *Esteve, Eduardo.* - “Los conflictos entre el derecho a la información y el derecho al honor en el Derecho comparado”, en *Revista de Derecho de la Universidad de Montevideo*, Año I, N° 1. UM. Montevideo (2002).

¹⁵ *Alexy, Robert.* - *Teoría de los derechos fundamentales*. Centro de Estudios Constitucionales. Madrid (2002).

¹⁶ Suitability, need, and proportionality in a strict sense are not weighted differently. It is not the case that sometimes one has precedence and other times it doesn't. The question is whether the partial maxims are satisfied or not, and if they are not, then the finding is illegal. Hence, the three partial maxims have to be cataloged as rules.

difficulties when the scope is more complex does not alter the deducibility of the nature of the principle, it only establishes its limits.”¹⁷

Duran argues that it is necessary to consider the proportionality test of Alexy, “but applying the proportionality in a strict sense from an orientation as to the values and purposes of the rights in play, with a view to reconciling them rather than ranking them in the form of a hierarchy.”¹⁸

“The weighting supposes three steps, which Alexy calls suitability, need, and proportionality in a strict sense.

Suitability refers to the appropriateness of the measure to achieve the proposed end. Once the suitability has been established, the next step is the maxim of need or minimal intervention. When this has been determined, the third step is to analyze the proportionality in a strict sense, which Alexy also calls “the mandate of proper weighting.”¹⁹

This mandate of proper weighting, according to Alexy, corresponds to the law of weighting, which states that “the greater the degree of non-satisfaction or involvement of the principles, the greater the importance of satisfying the other principle.”²⁰

This weighting is carried out by following three steps: “The first step is necessary to determine the degree of non-satisfaction or involvement of the principles. Then, in the second step, the importance of satisfying the principle that pulls in an opposing direction. Finally, in the third step, it must be determined whether the importance of satisfying the opposing principle justifies the application of the other principle”.²¹

This weighting is needed in situations involving colliding principles, which occurs in cases where two legal provisions are incompatible in principle. The weighting will be used to find a solution to this incompatibility.

It is possible that the conflicting principles are in a situation of equal hierarchical rank with respect to the statutory source of their content. However, one of them may prevail based on the consideration of the predominance of its value to society at any given moment.

It is important that the weighting provide some leeway to the people in charge of the interpretation, particularly with regard to choosing the preponderance of its value in contrast to the involvement of the principles. Subjectivism is a constant, as are the valuations carried out by the judges and the other persons involved. These valuations are the key factors on which the eventual legal decisions are based. While the weighting implies applied rationality, this does not mean that subjectivity can be avoided in the judge’s decision.

In this regard, the constitutional jurisprudence of some countries gives greater weight to the freedom of information, as opposed to the right to privacy or the right to dignity, given its inextricable association with the democratic conception of the Rule of Law, whereas other countries give greater weight to the right to privacy, valuing its association with the dignity of human beings.

Jurisprudence on this subject is manifested in several courts; the European Court of Human Rights in the case of *Guerra v. the Italian State*, found that “the Italian State had violated the right to private and family life by failing to provide the homeless with essential information that would have allowed them to assess the risks they and their families faced by remaining in Manfredonia, a city particularly vulnerable to the dangers of an eventual accident in a fertilizer factory. The European

¹⁷ Idem 15.

¹⁸ *Durán, Augusto*.- Derecho a la protección de datos personales y acceso a la información pública. Amalio Fernández. Montevideo (2009).

¹⁹ Idem 18.

²⁰ Idem 10.

²¹ Idem 18.

Court decided that exercising the right to private and family life requires not only that the State abstain from undue interference, but that the State also has the obligation to provide and disseminate information about environmental factors that could cause injury when this right is exercised. Only after this obligation has been fulfilled and the people are fully aware of the dangers or disturbances they may face, can the individuals involved decide whether or not they shall continue their residence at this place.”²²

In the case of Caffaro, C 265/07, the European Court of Justice found that “the aim of Directive 95/46/CE is that Member States, while allowing for the free circulation of personal information, must, nonetheless, ensure the protection of the freedoms and fundamental rights of natural persons, and, in particular, the right to privacy with regard to the processing of such information.”²³ It also states that this objective is impossible to achieve without reconciling it with other fundamental rights, such as the freedom of expression, which aims to reconcile two fundamental rights, the right to privacy and the freedom of information.

Continues, “to obtain a balanced weighting of the two fundamental rights, the protection of the fundamental right to privacy requires that exceptions and restrictions to information protection established under the Directive fall within the limits of what is strictly necessary. This requires taking into account that the exemptions and exceptions provided in Article 9 of the Directive apply not only to media companies, but also to any person engaged in journalistic activity. ... The fact that personal information is published for profit does not exclude a priori that it might be considered an activity “solely with journalistic purposes.” ... One has to consider the changes, the proliferation of the media, and the dissemination of information.”²⁴

4.3. How to solve the “problem”?

As Risso Ferrand has established, both specific cases and general claims have slowly led to the formulation of various rules, techniques, and criteria, some of which are highly useful, that can be used to help solve this problem.

The first step should always be an attempt to reconcile the conflicting rights. This is based on the fact that all human rights are essential and inherent to human beings, so that whenever a case entails sacrificing a fundamental right, one must realize that something of unusual gravity is occurring. All human rights, without exception, serve to regulate the higher values of the community (national and international) and the main objective of enforcing a certain right must always be to safeguard all of the rest of them without exception. Of course, the reconciliation process is not simple, but there are some tools that can help with the task:

First of all, reconciliation must always involve safeguarding the “essential content” of each of the rights in play, while avoiding the distortion of any of them.

Secondly, every possibility of analysis of the case in question must be studied thoroughly and exhaustively. Often the difficulties of reconciliation are more apparent than real and when all the components and nuances of a case are carefully examined and the proper distinctions are made, one often finds that reconciliation is indeed possible.

Above all, partial visions or biased perspectives of the problem (in favor of any of the values involved) must be avoided, since all human rights are equally valued and respond to higher values. These cases must be resolved by viewing human rights as a comprehensive set of rights that must

²² *Corte Europea de Derechos Humanos.- Caso Guerra vs Italia*, Sentencia de 19 de febrero de 1998.

²³ *Corte Europea de Derechos Humanos.- Caso Caffaro Srl vs Azienda Unità Sanitaria Locale RM/C*, Sentencia de 11 de setiembre de 2008.

²⁴ *Idem* 23.

be analyzed with a view to the overall system and with interpretive techniques suitable to the particular type of statute.

Stated more basically, the interpreter must resolve these cases by acting in defense of the system of human rights, and not according to political or ideological ideas. Avoiding this is not easy, but it must be done.

As Díez Picazo states, one must bear in mind that these techniques, in contrast to those that are subsumed, do not respond in terms of “yes” or “no”, but rather in terms of “more” or “less”, and the result will normally not be the primacy of one value over others, but rather reaching a point of equilibrium between the rights in question.

The vast majority of human rights cases in conflict or opposition can be resolved under the above-mentioned rule of reconciliation. However, there are cases in which such reconciliation is not possible. For these, one will have to resort to other means to find a resolution, but always bearing in mind that human rights form a singular fundamental unit, and that all of the rights must be protected. However, when this is not possible, each separate case will have its own particular solution.

In such cases, the principle of proportionality, which was originally developed by German jurisprudence at the end of the 19th century and is today accepted in practically all of Europe and a large part of Latin America, can be a great help. This principle was developed and employed to control the actions of public authorities and not to resolve conflicts between rights: but in spite of this, its use, although not definitive, serves to further the analysis of conflict and to approach a solution. In this regard, it is useful to refer to Alexy and, after that, to distinguish the margins for establishing the ends and the means for weighing the situation with three successive analyses.

First of all, one must analyze the suitability of sacrificing a right in order to achieve the sought-after ends (protection of the other interests at stake). Only when a relationship of suitability is found can one move forward with the analysis. In cases where rights are in conflict, no restrictions are acceptable if there is no suitable means of satisfying the opposing interest.

If suitability can be established, the next question to be asked is whether the sacrifice of one of the rights is absolutely necessary to achieve the sought-after aim, or if another way can be found to surmount the situation without sacrificing that right. If sacrificing the right is not absolutely essential to achieving the aim, or if there is an alternative that is less injurious to the restricted right, one must opt for the less injurious alternative. The solution based on reconciliation is always preferable.

Once the suitability and the need to restrict the right have been established, one must pass on to the subcomponent of the weighting in the strict sense, which consists of three steps: i) the degree of non-satisfaction of an interest (the sacrificed right) must be determined; ii) then, the importance of satisfying the opposing interests must be determined; and, finally, iii) the importance of satisfying the interests of the various rights at stake must be determined by means of weighting in a strict sense.

And lastly, the third rule states that for exceptional cases in which reconciliation is not possible (first rule) and the primacy of one right (value) over another right (second rule) must be determined, even after the final conclusion one must conduct another analysis of the case to determine if there are any other possibilities, however minor they may appear to be, that have been overlooked and that can to some extent safeguard the right that was sacrificed. This is not a minor issue, for if it has been concluded that the only possible solution is to sacrifice a right, the least that one can do is to make every effort to mitigate and justify such a sacrifice. ... It might be said that little is gained by

doing this, but it at least makes the sacrifice of something quite grave —the limitation of a human right— more bearable.²⁵

“The primacy of one right or another – if there is one – is never absolute, because, among other reasons, of the permanent validity of the principles of indivisibility and interdependence. These principles demonstrate that human rights form an axiologically complete system. They are not a set of separate pieces that can be disarticulated from one another in function of the attacks that some of them may come under. This is clearly seen when any human right is violated, because it invariably involves bringing injury to the dignity of a human being (Faúndez).

The underpinning and widespread recognition of the value of “human dignity” has led to the argument that all human rights are important and systemically interrelated. As an inevitable consequence, all human rights are necessary and justice should be sought for all of them, including economic and social rights. There is no a priori precedence of some over others. All conflicts must be dealt with on a case-by-case basis. Without a doubt, human rights form a comprehensive and indivisible system. This is a fundamental appraisal that has inspired numerous decisions of the Inter-American Commission on Human Rights and the European Court of Human Rights (Faúndez).”²⁶

5. References

Alexy, Robert.- Teoría de los derechos fundamentales. Centro de Estudios Constitucionales. Madrid (2002).

Bauzá, Marcelo.- “Criterios para armonizar la protección de datos personales y el acceso a la información pública”, en Anuario de Derecho Informático N° X. Fundación de Cultura Universitaria. Montevideo (2010).

Bobbio, Norberto, y otros.- Diccionario de Política. Siglo XXI Editores. México DF (1988).

Camou, Antonio.- Gobernabilidad y Democracia. Cuadernos de Divulgación de la Cultura Democrática N° 6. IFE. México DF (2001).

Camou, Antonio.- Los desafíos de la gobernabilidad: estudio premilitar. Editorial Plaza y Valdés. México DF (2001).

Carrillo, Fernando.- “El déficit de democratización en América Latina”, en Democracia en déficit: Gobernabilidad y Desarrollo en América Latina. BID. Washington (2001).

Corte Europea de Derechos Humanos.- Caso Guerra vs Italia, Sentencia de 19 de febrero de 1998.

Corte Europea de Derechos Humanos.- Caso Caffaro Srl vs Azienda Unità Sanitaria Locale RM/C, Sentencia de 11 de setiembre de 2008.

Dethier, Jean.- Governance and Economic Performance: A Survey. Discussion Papers on Development Policy. Center for Development Reserch. Bonn (1999).

Durán, Augusto.- Derecho a la protección de datos personales y acceso a la información pública. Amalio Fernández. Montevideo (2009).

Dworkin, Ronald.- Los derechos en serio. Editorial Ariel. Barcelona (1993).

Esteva, Eduardo.- “Los conflictos entre el derecho a la información y el derecho al honor en el Derecho comparado”, en Revista de Derecho de la Universidad de Montevideo, Año I, N° 1. UM. Montevideo (2002).

Ferrajoli, Luigi.- Derecho y razón. Editorial Trotta. Madrid (2005).

²⁵ *Risso, Martín*.- Algunas garantías básicas de los derechos humanos. Fundación de Cultura Universitaria. Montevideo (2011).

²⁶ *Idem* 13.

Lowenthal, Abraham.- “Latin America at the Century’s Turn”, en Journal of Democracy N° 11 Volumen 2. The Johns Hopkins University Press. Baltimore (2000).

Nogueira, Humberto.- Dogmática de los derechos esenciales.
<http://www.bibliojuridica.org/libros/3/1094/16.pdf>

Risso, Martín.- Algunas garantías básicas de los derechos humanos. Fundación de Cultura Universitaria. Montevideo (2011).

Sen, Amartya.- El desarrollo como libertad. Editorial Planeta. Barcelona (1999).

HABEAS DATA AND DATA PROTECTION LAW IN CHILE

Romina Garrido Iglesias

Lawyer, Library on National Congress of Chile, Legal Resources Area.
Huérfanos No. 1117 of. 209. Santiago, Chile.
rgarrido@bcn.cl, romina.garrido@gmail.com, www.protecciondedatospersonales.cl

Keywords: *Data protection, Chile, Law 19.628, Latin America, Habeas data.*

Abstract: *This paper shows a brief overview of data protection in Latin America and over the current Chilean law with its shortcomings, which need urgent reforms over the "data protection system" in Chile, not enough efforts being partial to today.*

1. Introduction

Today, the protection of data privacy is a key issue and one of significant international importance, not only due to the increasing diffusion of data throughout the internet but also due to the need for collaboration between domestic and foreign public bodies or companies when making decisions that fulfil their purposes and deliver the greatest benefits to their users. In this context it is necessary not to restrict access to data in the fear that data protection or confidentiality of information can't be guaranteed.

In modern legislation the protection of personal data is recognised by the right to privacy or autonomy. With the rise of computing, a new relationship between people and data has formed that needs to be protected beyond the rules concerning this right, and it is necessary that there is an explicit constitutional guarantee safeguarding personal data.

A key issue is of trust in sources of information, and data protection is a tool that gives us a standard of trust based upon the guarantee of our rights. Therefore, robust legislation on data protection is key for those who must make decisions based on information generated by data.

2. A look at Latin America

In Latin America, the protection of personal data has developed some of its own characteristics. Although the countries with the highest growth of law in this regulatory area have based their standards on the European model, it is not possible to ignore the particularities of the challenges to data protection that we are presented with. Assuming that there isn't, as in the European model, a Latin American law to data protection, the institution of *Habeas Data* highlights that the law has its own characteristics depending on the national approach. Data protection is relatively new in Latin America and the authors justify this delay mainly due to the comparatively late technological penetration in the region, since as mentioned, the protection of data constitutes a reaction to the automation of personal data, something which was not perceived on this scale in America.¹

¹ Artemi Rallo Lombarte, Ricard Martinez Martinez, Agustín Puente Escobar, Irene Agúndez Leria. Course: Right to Data protection. 3rd edition CEDDET. Chapter 6: The data protection and habeas data in Latin-American. National boundaries and approaches.

There is also a different approach to state intervention in the collection and treatment of personal information and data, which instead of being associated with a risky activity, conveys the impression that the state is concerned for its citizens giving the handling of data by the state a positive bias. Within this treatment of data is immersed the idea that the state is looking to improve the living conditions of citizens, which requires a greater use of personal data in government often supplied by the citizens themselves. On the other hand, it is notable that there are also public security imperatives, which are used to justify various forms of data collection and monitoring.

During the 1970s whilst the concept of data protection was in evolution in Europe, the issue went virtually unnoticed in America as it was in its initial phase of development. This development was namely the right of access to data, which led to *Habeas data*, which in turn is linked to the end of societies being governed under military regimes where much trauma was caused by the authoritarian use of information as an instrument of political repression.

It is possible to systematize the law of *Habeas Data*, stating the following:

- Brazil was the first country where Habeas Data was used as a resource to ensure the right of citizens to access and correct their personal data held by third parties. After Brazil, Habeas data was adopted in Argentina, Colombia, Ecuador, Guatemala, Paraguay, Peru, Uruguay and Venezuela.
- In Peru, the Constitution, as amended in 2005, provides in Article 2.6 that “*Every person has the right to assurance that information services, whether computerized or not, either public or private, will not provide information affecting personal and family privacy.*”²”
- In Venezuela, the Constitution of the Bolivarian Republic of Venezuela 1999, Article 60, states: “*Everyone has the right to protection of his honour, privacy, intimacy, self-image, confidentiality and reputation. The law will limit the use of information technology.*”³”
- In Colombia, Article 15 of the Constitution provides that: “*Every individual has the right to personal and family privacy and to his/her good reputation, and the state will respect them and have these rights and ensure they are respected. Similarly, individuals have the right to know, update, and rectify information gathered about them in data banks and in the records of public and private entities. Freedom and the other guarantees approved in the Constitution will be respected in the gathering, handling, and circulation of data.*”⁴”
- In the Constitution of Ecuador 1998, Article 66 N° 19 provides that: “*Every person has the right to protection of personal data, including access to the documents, databases and reports on themselves, or their property, recorded in public or private entities, as well as to know the use made of them and their end purpose.*”⁵”
- In Guatemala, the protection refers exclusively to the records that are held in state agencies, since Article 31 of the Constitution states: “*Every person has the right to know what the archives, records, or any other form of State registers contain about him and the purpose for which such data is used as well as their correction, rectification, and bringing up to date [actualisation]. Registers and records of political affiliation, except those pertaining to the electoral authorities and political parties are prohibited.*”⁶”

² Political Constitution of Perú. [Consulted 03.03.2014 <http://www.tc.gob.pe/legconperu/constitucion.html>]

³ Constitution of the Bolivarian Republic of Venezuela, 1999 [Consulted 03.03.2014 <http://www.tsj.gov.ve/legislacion/constitucion1999.htm>]

⁴ Political Constitution of Colombia 1991 [Consulted 03.03.2014 <http://pdba.georgetown.edu/constitutions/colombia/col91.html>]

⁵ Political Constitution of Ecuador 2008 [Consulted 03.03.2014 http://www.oas.org/juridico/PDFs/mesicic4_ecu_const.pdf]

⁶ Political Constitution of Guatemala. 1993. [Consulted 03.03.2014 http://www.oas.org/juridico/MLA/sp/gtm/sp_gtm-int-text-const.pdf]

- In Nicaragua there is a similar law for state authorities, where Article 26 N° 4 of the Constitution states that: *“All persons have the right to privacy and the privacy of their family; the inviolability of their home, correspondence, and communications of all kinds; to know all information about them registered by the state authorities, as well as the right to know why and for what purposes they have that information.”*⁷
- In the United States of Mexico a constitutional amendment in 2009 amended article 16 of its Constitution, stating: *“Everyone has the right to enjoy protection of their personal data, and to access, correct and cancel such data. Everyone has the right to oppose disclosure of his data, according to the law. The law shall establish exceptions to the criteria that rule the handling of data, due to national security reasons, law and order, public security, public health, or protection of third party’s rights.”*⁸

Aside from the delay concerning the issue of data protection in the region, in recent years many countries have based their data protection regulations on the standard that the European Union requires. In this regard, Chile was the first country to do so in 1998, and was later followed by Argentina in 2000 under law No. 25.326⁹, which created the National Personal Data Protection law and later obtained the declaration that the country was conforming to European standards in 2003. In turn in 2008, Uruguay made law No. 18.331¹⁰, which created the Regulatory Unit and Control of Personal Data and obtained the adequacy to the European standard via the decision of the European Commission on the 21st of August 2012¹¹.

Other countries that have only made law on data protection include Peru under their law No. 29.733 in 2011, Costa Rica under their law No. 8.968 in 2011 and finally Mexico in 2010 with the Federal Law on Protection of Personal Data in Possession of Individuals, to name a few.

3. A look at data protection in Chile

In Chile data protection is recognised as an implicit constitutional right through the right to privacy, which is enshrined in the Constitution of 1980 in Article 19 No. 4 that guarantees every person *Respect for and protection of private and public life* and the honour of the individual and his family.¹²

Before this text it should be noted that there was no expressed right on the protection of private life until the Constitutional Act No. 3, which was passed on September the 18th 1976 and replaced the constitutional guarantees that were effective under the Constitution of 1925, being the direct precursor of the protection of privacy of the private life. Whilst the discussion of this right was held in conjunction with the inviolability of private communications, it is possible to understand from

⁷ Political Constitution of Nicaragua 1986. [Consulted 03.03.2014 <http://www.ineter.gob.ni/Constitucion%20Politica%20de%20Nicargua.pdf>]

⁸ Constitution of United States of Mexico
[Consulted 03.03.2014 <http://info4.juridicas.unam.mx/ijure/fed/9/17.htm?s=>]

⁹ Ley No 25.326 [Consulted 03.03.2014 <http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>]

¹⁰ Ley No 18.331. [Consulted 03.03.2014 <http://www.parlamento.gub.uy/leyes/AccesoTextoLey.asp?Ley=18331>]

¹¹ Adequacy determination from EU for personal data protections
http://www.agesic.gub.uy/innovaportal/file/2303/1/adequacion_ue.pdf

¹² Before the constitutional reforms of 2005, introduced by Law No. 20.050 this article also protected public life and stated that the infringement of this provision, committed through a social media, and consisting in the implication of a false fact or act, or causing unwarranted damage or discrediting a person or their family, shall constitute a crime and the penalty will be determined by law. However, social media could be exempt by proving to the corresponding court the truth about the implication, unless it itself causes the crime of injury to individuals. In addition, the owners, editors, directors and administrators of the respective social media will be jointly responsible for relevant compensation.

the constitutional records that the need existed to recognise the right to privacy that was already regulated in the Declaration of Human Rights and American Declaration of the Rights and Duties of Man and other countries in the region and the European continent.¹³

Within this constitutional right the Chilean legislator implicitly recognised the guarantee of *protection of personal data* and the right and ability to control your own information against automated processing.

Alongside this there have been several legislative efforts oriented towards the recognition of the impact that technological change and developments have on making the law, and that it is necessary to expand the law and explicitly recognise the right to control data, as its illegitimate treatment can affect the most sensitive aspects of life. This is why people are starting to demand recognition of the issue and concrete defence mechanisms for the use and control of data.¹⁴

This provision is the framework of the development of the guarantee of data protection in Chile related to privacy. It was thought that the development of this law as a constitutional guarantee was set by law No. 19.628 in 1998, but in the legislative process the development of the law was not treated as a constitutional guarantee, which implies it was approved only under simple law. However, the state and the entities that carry out data processing are not only subject to the requirements of the constitutional provision that guarantees the respect and protection of privacy of individuals, but also to law No.19.628. In the same context, the justification for data processing by the state is born of its own means, which intends to create the social conditions that allow each and every one of the members of the national community to achieve the greatest spiritual and material fulfilment as possible, with full respect to the rights and guarantees which the Constitution establishes. A lack of information on people implies that there is an inability to promote the strengthening of the population, the harmonious integration of all sectors of the nation and to ensure the rights of people to participate equally in the opportunities in national life¹⁵.

As noted, since 1998 in Chile we have had specific legislation on the processing of personal data under law No. 19.628 on the Protection of Private Life. The intention of this law was to create a system of *civil protection* of the right to privacy, it was recognised that for the advancement of life in society the free flow of information is necessary, whilst always being handled carefully at the same time in reference to natural persons¹⁶.

The law was made in a context that in Chile it was necessary to legalise the market of the handling of personal data, particularly the data processed by the credit bureaus. During this legislative process companies interested in regulating the activity, in which personal data was their business capital, participated greatly.

Chilean law therefore establishes freedom for data processing, provided it is done in a manner consistent with the law and for purposes permitted by the law, always respecting the full exercise of the fundamental rights of the data holders, which the law affords them.

Protected legal entities in any legal system that has a data protection law, including Chile, have the freedom of computational or informational self-determination, so called computer privacy, covering

¹³ *Pedro Anguita Ramirez*. The data protection and the right to privacy. Analysis of the law 19.628. Chile Legal Editorial of Chile. 1 st edition, 2007. Pag 119.

¹⁴ One example is the Bill No. 5883-07, amendment to Law N°19.628 for explicit recognition as a fundamental right. [Online] Source: <http://sil.congreso.cl/cgi-bin/sil_proyectos.pl?5883-07> [Accessed 20 December 2011]

¹⁵ In this subject can be consulted *Considerations and Recommendations on the processing of personal data by public sector*. Rodrigo Gutierrez. Chile and Personal Data Protection: Are in crisis our fundamental rights? published by Series Public Policy Ediciones Universidad Diego Portales. Ed. Expansiva 2009

¹⁶ History of the law No 19.628. Motion of senator Eugenio Cantuarias Larrondo, 05 January 1993. <http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursoslegales/10221.3/2468/7/HL19628.pdf>

the reserve and control of personal information in order to ensure the preservation of identity, dignity and freedom, which has been called "*third generation rights*".

In the legislation in general there is a protection on the data so that it cannot be manipulated, and information can only be used for authorised purposes and by those authorised to do so. Chilean law, in this sense does not meet the standard because it does not contemplate the principle of the dual nature of control: the right of the data holder to control the processing of data, and the existence of an independent public body that monitors the activity of those who process data and have powers of intervention, investigation, surveillance and punishment¹⁷.

Law No. 19.628, as a framework regulates the activity of data processing generically applicable to the public and private sector when performing a data processing activity.

The principles of data protection, to which many authors have referred to at some length, are set forth in the law. From the law there are guidelines for the legal processing of data, but a lack of control results in the absence of an effective system of guarantees, which is the main shortcoming of the law.

The law then, gives us the legal framework for the state and for individuals when they process data, but does not include monitoring and sanctioning mechanisms against illegal data processing that are effective and allow both the people responsible for the databases and for the data owners to be aware of the risks that the illegal handling of data represents, which is the effect on fundamental rights.

Objects of the law that are generally regulated and applicable to the case of data processing by public agencies are on one side personal data and on the other side the data held at a bank or on a public register. The law defines personal data as that relating to any information concerning an identified or identifiable natural person, and bank data or data on a public register as an organised set of personal data, which can be automated or not, and any form or mode of organisation that allows data to relate to other data as well as preform all processing of data. This definition is certainly applicable to a database or register maintained by a state or private agency.

The law regulates data processing by public and private agencies outlined in the Constitution and those set out in Article 1 of the General Basis of State Administration and public services and bodies created to perform administrative work in Chile. The liability rests on the agency or public body that processes data, those who assume the role of responsibility for the register or database i.e. who is responsible for the decisions related to the handling of personal data, and not only that it extends to any person working on personal data, who has the duty to maintain confidentiality or secrecy of the data and background information related to the database. This is an obligation that continues in spite of activities ending in this field, as long as the data doesn't come from or hasn't been collected from publicly available sources.

In addition, the law defines the operations of data processing, stating that data treatment is any operation or set of operations or technical procedures automated or not, enabling the collection, storing, recording, organizing, developing, selection, extraction, comparing, interconnection, dissociation, communication, assignation, transfer, conveyance or deletion of personal data, or use of it in any other way. From the text of the law you can also extract principles and basic rules of data processing.

According to Law No. 19.628, the processing of personal data can only be done when the law itself or other legal regulations authorise it or the owner gives expressed consent as stated in article 4 of

¹⁷ In fact, in the VI Ibero-American Data Protection meeting in Cartagena de Indias, May 29, 2008, Thomas ZERDICK, LL.M. Comisión Europea from the Direction of General Justice, Freedom and Security, submitted 9 simple steps to adequacy and the first of them refers to this dual control..

the law in general, followed by numerous exceptions that eventually become the general rule. As for the state, the rule is that it only processes data within its jurisdiction and subject to the rules that the law No. 19.628 specifies, and only under these conditions do not need the consent of the owner.

Conversely, if the public body is handling data outside the scope of its competence, the data owner must authorise such processing and should be properly informed about the purpose of storing personal data and its possible communication to the public. The law states that the person authorising must authorise in writing. The authorisation may be revoked but without retroactive effect, and must also be in writing.

In terms of the purpose of data use, the law rules that personal data must be used only for the purposes for what it has been collected, except from when it comes from or has been gathered from public sources. The entities that process data may establish automated transmission procedures, provided that the rights of the data holders are safeguarded and that the transmission is related to the duties and objectives of the participating agencies. The law states that the recipient of the personal data transmitted can only use the personal data for the purposes that were intended by the transmission.

With regards to the duty of confidentiality, as mentioned above, the people working in the processing of personal data both in public and private agencies are sworn to secrecy if the data comes from or has been gathered from publicly unavailable sources, or from other data and records related to databases. This is an obligation that continues in spite of activities having finished in that field.

Due diligence in the processing of data is also a principle in the law, stating that *"The responsible for the databases or registers that store personal data should take care of them with due diligence after its collection, taking responsibility for the damage."*¹⁸ Regarding the quality of the data, the law states that the information contained in the database must be accurate, up to date and truthfully reflect the real situation of the owner of the data. Personal data must be deleted or cancelled when it is stored without substance legal or if it has expired. Data should be changed when it is wrong, inaccurate, misleading or incomplete. Personal data where accuracy cannot be established or where validity is doubtful and for which cancellation is not appropriate will be blocked. The responsible of the personal information database shall eliminate, modify or block data where appropriate without request of the owner.

In respect of data security, there is no express mention of this in the law. However, it is possible to argue that since the obligation to establish the traceability of transmitted data exists, there exists an obligation to implement security measures¹⁹. There is no express mention of the security levels required according to the categorisation of the databases, which leaves it up to the good practice of organisations to manage this.

It is important to note that the rules outlined on data consent and security do not apply in the case of personal data accessible to the general public or when transmitting personal data to international organisations in compliance with the provisions in treaties and conventions in force. There isn't a clear reason for the first exception. As for international treaties, once they are ratified, they become part of the national legal system and assume the value of laws of the Republic. Regarding publicly accessible source, defined as records or personal data collections, public or private, with

¹⁸ Article 11 Law No 19.628. <http://www.leychile.cl/Navegar?idNorma=141599&idParte=8642693&idVersion=2012-02-17>

¹⁹ Article 5 Law N° 19.628 <http://www.leychile.cl/Navegar?idNorma=141599&idParte=8642687&idVersion=2012-02-17>

unrestricted access or access reserved for applicants, it is questionable because ultimately we could reach the conclusion that the owner of the database determines its accessibility.

Chilean law recognises data holders, only natural persons, and consecrates them in a system we call "*Habeas Data Law*"²⁰ regarding the right of access to data. Beside that the system regulates the exercise of the right to delete, block and free data in all operations related to data processing.

The right of access to information can be exercised in the body holding the database, or if it is a database which can be accessed by various agencies the owner of the data may request information from any of them. The access also involves the right to know what data is processed, its origin and recipient, the purpose of storage and identification of the persons or bodies to which the data is transmitted regularly.

As for the right of modification, deletion and blocking of data, the standard states that if the personal data is incorrect, inaccurate, misleading or incomplete and is credited as so, it shall be entitled to be modified. Regardless of legal exceptions, data may also be required to be removed in the cases where its storage lacks a legal basis or when it has become outdated.

In instances where the responsible for the database fails to deliver the copy or do any rectifications or deletions needed, people have the right to go to the local judge, so that he can rule on the respective amendments. This is enshrined in Habeas Data, so that the data owners know why and under what legal basis data is processed.

As illustrated the law provides many guarantees, but often lacks the effective tools and procedures to address any violations, and this is the biggest problem. The procedure that was established by law is handled by the civil courts, and until this day, 15 years since its validity, it has not had a big, concrete, practical application. Current legislation has considered the use of specialised entities to deal with the violations of this law, who could also scrutinise and oversee those processing the data. The procedure of Chilean Law is not consistent with the current technological reality and the weight of the burden of proof is on the victim. In short, when we examine the costs and benefits of the exercise of the Habeas Data legal action, given that it doesn't have concrete and effective sanctions, has to be exercised as any common lawsuit in court and the cost of the legal defence is on the data owner, the data owners are discouraged from exercising it. There is a complete lack of a controlling authority in any way.

4. Need for legislative change

The attempt to remedy the precarious situation of the Chilean Law has resulted in the presentation of diverse legislative initiatives with new systems of regulation, fortunately none of which have been successful despite Chile's international commitments to the matter.

I say fortunately in the first place because none of the legislative initiatives recognise a model or system that suits a standard of protection of fundamental rights, which mean that none of them considers a unique, specialised, independent, supervisory authority with the power for example to control it and punish those who do not adhere to it. Secondly, nobody has tried to look at the issue based upon what constitutes appropriate protection for the Chilean reality, there are only copies of the European system, or bodies that are created with various functions and skills that have been recycled. However, there have been a few advances, particularly in response to the indiscriminate abuse of databases containing personal economic, financial, commercial and banking data. Law No. 20,575²¹, made in February 2012, established *the principle of finality* in the treatment of these

²⁰ Indeed so enshrined in Article 12 of Law N° 19.628

²¹ Law N° 20.575 <http://www.leychile.cl/Navegar?idNorma=1037366>

databases, which was already recognised in Law No. 19,628 but needed redefining given the arbitrary behaviour of that specific market.

Another change, tangential to the subject, occurred in 2008 with the formation of Law No. 20,285 on Access to Public Information, which created a specialised body on this matter, namely the Council for Transparency, which was given power by law to “ensure proper implementation of Law No. 19,628, of the protection of personal data, on behalf of the organs of the Administration of the State”. When reviewing the true history of the law²², you don’t get to understand why the legislature gave the Council a power as extensive as described. In that same year there was a legislative attempt that failed and has done until today to modify the Council’s powers, and assign direct authority on data protection in public agencies, stating that:

"It was necessary to meet the requirements of the protection of the right to informative self-determination, and coupled with the realisation that the establishment of a supervisory authority is critical to actual law enforcement was the need to incorporate powers stated in this directive within the competence of the Council for Transparency during the parliamentary discussion of the law N ° 20,285. However, it was only given the power to “Ensure proper implementation of Law No. 19,628, of the protection of personal data, on behalf of the organs of the Administration of the State”. There was awareness that it would be insufficient for the protection of the processing of personal data and the rights of the data owners. But it was agreed to advance and deepen the current regulation.”²³

With the publication of the Law on Transparency and Access to Public Information under Law No. 20,285 in 2008, the constitutional principle of the transparency of the public sector was recognised in practice. Together with it the right of access to information and the procedures for the exercise of the law and for its protection were also established, with the exceptions to the disclosure of information being those which could infringe on people’s rights, particularly in the case of their safety, health, private life or commercial and economic rights.

It follows then that Law No. 19,628 on data processing and Law No. 20,285 on access to information provide the general framework for the processing of data by the public sector, considering that in the context of transparency law state information is public in nature, and there is therefore a legitimate desire that it should be made available and accessible to the public. Both laws are essentially a balance of the same situation. This is regarding how to deal with this data, the rights of the holders and the access limitations when the information requested includes personal data of third parties.

In any field it is necessary to form a balance, and in the public sector we need legislation that weighs the harm caused by privacy violations against what is in the public interest. This proportional assessment corresponds today to a weak framework of privacy on the data held by state agencies. In the private sector the objective is to create a harmony between the free flow of information and the right of control over your own data, which today in Chile is attributed to the “goodwill” of those who are responsible for private databases and who understand that data protection helps to generate confidence in new technologies. Overall, the processing of data with respect to fundamental rights is a challenge for public entities and for all organisations.

²² History of law No 20.285

<http://www.leychile.cl/Navegar/scripts/obtienearchivo?id=recursolegales/10221.3/506/1/HL20285.pdf>

²³ Amendment bill Law No20.285. Executive Message to Chilean Congress
http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=6120-07

5. References:

Artemi Rallo Lombarte, Ricard Martinez Martinez, Agustín Puente Escobar, Irene Agúndez Leria. Course: Right to Data protection. 3rd edition CEDDET. Chapter 1: The protection of personal data. Basic concept.

Artemi Rallo Lombarte, Ricard Martinez Martinez, Agustín Puente Escobar, Irene Agúndez Leria. Course: Right to Data protection. 3rd edition CEDDET. Chapter 6: The data protection and habeas data in Latin-American. National boundaries and approaches.

Pedro Anguita Ramirez. The data protection and the right to privacy. Analysis of the law 19.628. Chile Legal Editorial of Chile. 1 st edition, 2007.

Rodrigo Gutierrez. Considerations and Recommendations on the processing of personal data by public sector. Chile and Personal Data Protection: Are in crisis our fundamental rights? published by Series Public Policy Ediciones Universidad Diego Portales. Ed. Expansiva 2009

Digital resources:

Political Constitution of Perú.

Consulted 03.03.2014 <http://www.tc.gob.pe/legconperu/constitucion.html>

Political Constitution of Venezuela. 1999.

Consulted 03.03.2014 <http://www.tsj.gov.ve/legislacion/constitucion1999.htm>

Political Constitution of Colombia. 1991.

Consulted 03.03.2014 <http://pdba.georgetown.edu/constitutions/colombia/col91.html>

Political Constitution of Ecuador 2008.

Consulted 03.03.2014 http://www.oas.org/juridico/PDFs/mesicic4_ecu_const.pdf

Political Constitution of Guatemala. 1993.

Consulted 03.03.2014 http://www.oas.org/juridico/MLA/sp/gtm/sp_gtm-int-text-const.pdf

Political Constitution of Nicaragua 1986

Consulted 03.03.2014 <http://www.ineter.gob.ni/Constitucion%20Politica%20de%20Nicargua.pdf>

Constitution of United States of Mexico

Consulted 03.03.2014 <http://info4.juridicas.unam.mx/ijure/fed/9/17.htm?s=>

Argentina, Law No 25.326

Consulted 03.03.2014 <http://www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/norma.htm>

Peru, Law No 29.733

Consulted 03.03.2014 http://www.informatica-juridica.com/anexos/Ley_29733_2_julio_2011_Proteccion_Datos_Personales.asp

Costa Rica, Law N° 8.968

Consulted 03.03.2014 http://www.informatica-juridica.com/anexos/Ley_8968_Proteccion_persona_frente_tratamiento_sus_datos_personales.asp

Chile, Law N°19.628 and related resources.

<http://www.leychile.cl/Navegar?idLey=19628>

Chile, Law No 20.285 and related resources.

<http://www.leychile.cl/Navegar?idNorma=276363>

Chile, Law 20.575 and related resources

<http://www.leychile.cl/Navegar?idNorma=1037366>

CHALLENGES OF INCREASED INTERNATIONAL DATA EXCHANGE: POLICE/SECURITY SERVICES & FINANCIAL TRANSACTIONS

Erich Schweighofer^{*} 

Professor, University of Vienna, Centre for Computers and Law
Schottenbastei 10-16/2/5, 1010 Wien, AT
erich.schweighofer@univie.ac.at
<http://rechtsinformatik.univie.ac.at>

Keywords: *International data exchange, data protection, smart surveillance, prevention of crimes, law enforcement, police cooperation, financial transactions, fundamental rights*

Abstract: *In our globalised world, and especially in Europe, borders do no longer have the same meaning as twenty years ago, even less so considering the “cyberspace”. The benefits thereof are however accompanied by criminal threats which are increasingly met by international police cooperation. In this regard the cross-border exchange of information between security services and financial institutions is one of the central tasks. This paper shall give an overview of existing “smart” surveillance tools as well as surveillance of financial transactions and the need for a stronger regime on international data exchange. Short overviews on the related FP7 Research projects SMART and RESPECT are added.*

1. Cyberspace and smart surveillance

At least since the growing cybercrime, cyberspace is considered even by sceptics as a challenge to modern lawyering, in particular in national and international security. Due to the September 11 attacks, surveillance has got a very high priority in national and international security efforts.¹ Surveillance² is a method of social control and means matching over the behaviour of people, e.g. monitoring their activities and behaviour. The purpose can be very different, from protection to exercising influence. Modern IT (e.g. electronic equipment) has greatly enlarged such possibilities and significantly reduced costs (CCTV cameras, Internet traffic, phone calls, financial transactions etc.). An analysis of public surveillance powers needs to consider two basic premises: Firstly, every constitutional democracy guarantees a basic order where everybody shall have equal rights and freedoms that protect every individual's human dignity and self-determination, whereas these spheres of freedom have to be respected mutually. Secondly, it is implicit within the social contract that the enforcement monopoly³ is allocated to the State, acting through its civil servants, in order to secure these spheres of freedom. Hence a certain amount of control over the people serves a

^{*} The author is indebted to input from the FP7 research projects SMART and RESPECT and the related articles and presentations at the conferences IRIS2012 (Ch. Tschohl, E. Schweighofer, W. Hötendorfer, M. Schrems), IRIS2014 (J. Böszörményi, E. Schweighofer) and CPDP2014 (E. Schweighofer, W. Hötendorfer).

¹ Wikipedia EN: September 11 attacks (last accessed: March 31, 2014).

² Wikipedia EN: surveillance (last accessed: March 31, 2014).

³ This term was particularly formed by Weber, M., *Wirtschaft und Gesellschaft*. Grundriss der verstehenden Soziologie, § 17 (1922); online available at http://www.textlog.de/weber_wirtschaft.html last accessed 9.2.2012 (2006).

legitimate purpose, as far as such is *necessary in a democratic society and in accordance with the law*⁴.

Cyberspace⁵ or internet governance⁶ constitutes a new approach of governance in a globalized world.⁷ Internet governance is the leading example of the changing concept of sovereignty of States.⁸ The Westphalian system of 1648 with its strong emphasis on territorial sovereignty is slightly but continuously replaced by a more liberal approach.⁹ Globalization, efficient and cheap transport facilities and new forms of communication like the Internet have severely limited the importance of borders as long as the respective State participates in the existing international co-operation. It has become very difficult or even impossible for a State to cut itself off from the practice of other States.¹⁰ Digital boundaries can be established only at the cost of losing the advantages of international cooperation. However, effective control and selective blocking of trans-border communication is possible and constitutes an option, in particular for less democratic states. In this liberal system of sovereignty, territory will still play a major role but the human being and its rights are moving into the centre of international relations. A new transnational order will be established characterized by increased international networking of persons, private international organizations, commercial enterprises and various entities of government. The enhanced communication of government institutions of different States leads to a new form of mutual work-sharing and support in regulation. However, the State as the provider of internal and external security maintains a central role. The functions of adjudication and execution by the State are indispensable. A special cyberspace jurisdiction is out of discussion¹¹ but multi-level governance by States, international organizations, local government, transnational corporations, civil society groups, especially non-governmental international organizations will be or is already the standard.¹² Even if the difficult process of readjusting principles of territorial sovereignty, conflict of laws and

⁴ Compare Article 8 para. 2 Convention for the Protection of Human Rights and Fundamental Freedoms, CETS No. 005, Council of Europe, Rome, 4.11.1950, as amended (hereinafter: European Convention on Human Rights or ECHR).

⁵ A quite common description of cyberspace: It is the virtual world of computer networks that can be explored by anyone who has a computer and access to the network by modem or local network. Persons can visit computer systems all over the world and communicate with other computer users. W. Proksch, Internet Governance (Ph.D dissertation on file at the University of Vienna, 2003) distinguishes between internet governance as technical regulation and cyberspace governance as regulation of human behaviour in the global village. However, the Working Group on Internet Governance (WGIG) has chosen a broad definition blurring the difference between internet and cyberspace governance.

⁶ For a definition of governance see *UN Commission on Global Governance, Our Global Neighbourhood* (1995), <http://www.cgg.ch/CHAP1.html>.

⁷ The Working Group on Internet Governance on the World Summit of the Information Society (WSIS) has given a very broad definition of internet governance: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." Report of the Working Group on Internet Governance, <http://www.wgig.org/docs/WGIGREPORT.pdf>, 4.

⁸ Cf. H.H. Perritt, jr., The Internet as a Threat to Sovereignty: Thoughts on the Internet's Role in Strengthening National and Global Governance, 5 GLSJ 4 (1998), <http://www.law.indiana.edu/glsj/vol5/no2/4perritt.html>; H.H. Perritt, jr., The Internet and International Law, 88 Kentucky Law Journal 885 (1999/2000).

⁹ A.-M. Slaughter, International Law in a World of Liberal States, 6 EJIL 503 (1995).

¹⁰ W.B. Wriston, Bits, Bytes and Diplomacy, Foreign Affairs 172 (1997).

¹¹ Cf. J. Goldsmith & T. Wu, Who Controls the Internet, Illusions of a Borderless World (2006), L. A. Bygrave & J. Bing (Ed.), Internet Governance. Infrastructure and Institutions, Oxford University Press (2009). Earlier approaches are described in: D.R. Johnson & D.G. Post, The Rise of Law on the Global Network, in B. Kahin & C. Nesson (Eds.), Borders in Cyberspace, Information Policy and the Global Information Infrastructure, 3 (1997).

¹² C. Engel, *The Internet and the Nation State*, Preprints of the Max-Planck-Projektgruppe Recht der Gemeinschaftsgüter, Bonn (1999), http://www.mpp-rdg.mpg.de/pdf_dat/engel1.pdf; K.W. Grewlich, Governance in "Cyberspace", Access and Public Interest in Global Communications (1999); E. Schweighofer, A Review of ICANN's Uniform Dispute Resolution Policy. In: Austrian Review of International and European Law, Kluwer Law International, Vol. 6, 2001, 91-122 (2001).

self-regulation for cyberspace is still going on, modern law is already strongly characterised by this approach, including also regulation by IT (e.g. Lessing¹⁴ or now the strongly discussed Privacy by Design¹⁵ approach).

A contrast to the new freedoms of the internet is the growing surveillance of citizens. States are eager in developing and improving other forms of control in order to secure a sufficient level of enforcement of its rules. Besides increased international co-operation, the use of already existing or newly collected data remains a strong focus of States. Surveillance techniques, e.g. video surveillance, monitoring of communication data, automatic semantic web analysis, repositories of DNA and fingerprints etc., allow a systematic and large scale control monitoring of people on a scale as never before. Whereas a reasonable use for maintaining public order and the social contract should not be challenged, a strong danger exists that – at least for a while – these techniques will be used without sufficient regard to human rights, in particular to privacy.

In general, five different methods of international cooperation between administrations, in particular police/security forces, can be distinguished: direct communication between the central State offices, indirect communication via international platforms, e.g. INTERPOL, Europol and Schengen, also offering international databases, "small border communication" between officials from neighbouring countries in adjoining areas, and mutual access to databases such as foreseen in the Treaty of Prüm or in "Prüm-like" bilateral cooperation. All forms of data exchange are used according to the particularities of the relevant cases with growing importance of the European co-operation environment.

Smart" surveillance means any kind of investigation or control carried out by automatic means *and* providing for a certain use of artificial intelligence beyond techniques of knowledge management (establishment and use of structured or unstructured data repositories etc.). Some ontological structuring of data and (semi)automatic reuse are the keys to "smart" surveillance. In practice, no clear borders exist. Data mining and data matching are well known techniques considered as "smart" by practice. Data mining means a process of discovering particular new patterns and relationships in large volumes of data on the basis of pre-determined criteria where such a process is performed mostly automatically, and combines tools from statistics and artificial intelligence with database management to analyse large digital data sets.¹⁶ Data matching means a process of finding entries that refer to the same target across different data sources, cross-linking and/or joining different digital data sets that do not share a common identifier.

2. SMART and RESPECT projects

The SMART Project¹⁷ (Scalable Measures for Automated Recognition Technologies), funded under the EU's Seventh Framework Programme for Research (FP7)¹⁸ with a total amount of €3.5 Million, addresses the questions of automated decision taking with respect to the "smart surveillance" technologies, taking into account that privacy and data protection are fundamental rights in the

¹⁴ L. Lessing, *Code and Other Laws of Cyberspace* (1999). Software adds another form of governance to the existing complexity. Human behaviour may be guided, allowed or disallowed by software code constraining it as effectively as rules with sanctions. This new form of regulation is quite impressively described by Lessig as *code as code* (software code = law code).

¹⁵ Wikipedia EN: Privacy by Design (last accessed: March 31, 2014); A. Cavoukian, *Privacy by Design: 7 Foundational Principles* (<http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/>) (last accessed: 31 March 2014).

¹⁶ For a full definition of data mining and further details see e.g. Gupta, G.K., *Introduction to Data Mining with Case Studies*, Prentice-Hall of India, New Delhi (2006).

¹⁷ See the project website: <http://www.smartsurveillance.eu> (last accessed 31 March 2014).

¹⁸ For more details to this funding line see http://ec.europa.eu/research/fp7/index_en.cfm (last accessed 31 March 2014).

EU's society. The basis of smart surveillance systems is the automated recognition of individuals and/or pre-determined traits or risk factors/criteria. The SMART project combines a technical review of key application areas by sector with a review of existing pertinent legislation. The overall objective is to produce a set of guidelines and a model law compliant with data protection rules. Four distinct project streams exist: Status quo analysis, citizen attitudes, technology infrastructure and best practice. The research considers both the domestic level and the EU level. The project consortium consists of 20 partner institutions from fifteen countries across the European Union which groups nearly forty researchers, embracing public universities and private research institutions as well as practitioners such as Interpol.¹⁹

The RESPECT Project²⁰ (Expectations & Security through Privacy-Enhanced Convenient Technologies), funded under the EU's Seventh Framework Programme for Research (FP7)²¹ with a total amount of €3.5 Million, deals with the role of surveillance systems and procedures for the prevention and reduction of crime, for evidence gathering and the improvement of prevention of crime and acts of terrorism, the identification and examination of social and economic costs of surveillance systems and procedures. The legal frameworks for these systems will be analysed and best practices identified. The awareness and acceptance of surveillance systems and procedures of European citizens will be analysed concerning efficiency, economic and social costs, considering the possible effect of cultural influences. The findings of other FP7 projects (CONSENT, SMART, SURVEILLE, IRISS etc.) should be compared and further developed. Finally, a set of tools is developed in the form of a matrix-like check-list (as a decision support tool for policy committees) of operational, technical, economic and social factors as well as legal aspects, guidelines for the system design and a model law for police forces who want to use monitoring systems.²²

3. International data exchange

The Internet is the best metaphor for the change from the information society to the knowledge society and the network society²³. Nearly everything is now digital, e.g. represented in some formal structure or a searchable text in a data repository. The information and communication infrastructure has tremendously changed and thus also the potential for data exchange across borders.²⁴ The research in the SMART and RESPECT projects shows that police/security services of the EU-Member States have used the potential and greatly improved data collection, data repositories and interfaces for data exchange. The knowledge management is now impressive but also slightly disturbing. The capacity for data exchange between police forces has greatly increased and the role of intermediaries like INTERPOL has also changed to being more a platform of data exchange. Technical constraints are much weaker; the law is now the gatekeeper for the necessary safeguards for digital rights.

Police/security institutions follow the strategies of E-Government in Europe but also the aims and goals of the European Union, e.g. a closer and more effective European co-operation. Partly, the police/security services are using the same infrastructures and technologies.

¹⁹ The project coordinator is Joseph Cannataci from the University of Malta. Erich Schweighofer leads the team of Vienna University responsible for work package 7 regarding the "review of laws governing interoperability and data exchange between police/security services".

²⁰ See the project website: <http://respectproject.eu> (last accessed 31 March 2014).

²¹ For more details to this funding line see http://ec.europa.eu/research/fp7/index_en.cfm last accessed 7.2.2012.

²² The project coordinator is Joseph Cannataci from the University of Groningen. Erich Schweighofer leads the team of Vienna University responsible for work package 8 regarding the "Tracking of financial services".

²³ A. Saarenpää, Legal Informatics Today. The View from the University of Lapland. In this conference proceedings.

²⁴ T. Berners-Lee, J. Hendler, O. Lassila, The Semantic – Web A new form of Web content that is meaningful to computers will unleash a revolution of new possibilities, Scientific American May 2001, New York, 35-43 (2001); Legal XML (<http://www.legalxml.org/>).

Data collection is now strongly a public and private partnership. Police/security services have always relied on private data but now with the growing data collection in the private sector – very often supported or even ordered by the public sector, e.g. data retention in the telecommunications sector – it has become a major source of police information. It depends on the government structure and the legal constraints under which conditions the police/security services can use these data.

3.1. Communication networks in the police/security sector

Special networks for the police/security sector are the sTESTA (EU private networks) and INTERPOL's I-7/24 & I-Link. sTESTA is an important part of the interoperability architecture actions of the ISA programme (Interoperability Solutions for European Public Administrations).²⁵ It should support public administrations in providing efficient public services to businesses and citizens across Europe, focusing on efficient and effective cross-border electronic collaboration between European public administrations.²⁶

sTESTA (secured Trans European Services for Telematics between Administrations) is a European framework for secure networks dedicated to inter-administrative requirements. The Internet Protocols (IP) is used to ensure universal reach, but is operated separately from the Internet by the European Commission. Thus, sTESTA offers guaranteed performance, high levels of security connections with all the EU Institutions and national networks for both unclassified and classified information. The sTESTA framework is open for any application within public administration that requires a cross border exchange of information.²⁷ Each sTESTA network forms a separate private network and is protected by special crypto devices on the network level. The various routers of each S-TESTA network operate completely separate from each other. In each router a separate crypto-box is exclusively installed.

sTESTA has become the standard for communication between police/security services: SIS II, the second generation Schengen Information System, for maintaining and distributing information related to border security and law enforcement²⁹; the Prüm Convention for exchange data regarding DNA, fingerprints and Vehicle registration of concerned persons and to cooperate against terrorism; EURODAC, the database system for fingerprints of asylum applicants; VIS, the Visa Information System with the aim of preventing visa shopping and improving the possibility to return illegal immigrants; TACHONET, the communication infrastructure for exchanging information on Tachograph Cards for trucks; CECIS, the Civil Protection and Environmental Emergencies

²⁵ Cf. the ISA homepage: http://ec.europa.eu/isa/index_en.htm (last accessed: 31 March 2014).

²⁶ SMART Project, Deliverable D5.1, Overview of Smart Surveillance Technologies in e-Government (2012).

²⁷ Cf. the homepage of the ISA programme: http://ec.europa.eu/isa/actions/02-interoperability-architecture/2-4action_en.htm. The list of ISA actions is very long and impressive; those on trusted information exchange are in particular: Improving semantic interoperability in European Government Systems, improving cross-border access to government data, accessing Member State information resources at European level, EU-wide interoperability of electronic identities (ECAS-STORK integration), an interoperable solution for electronic signatures (eIDs – STORK sustainability), developing electronic procurement in Europe (PEPPOL sustainability), promoting the take-up of pan-European electronic procurement (e-PRIOR electronic procurement platform), permitting secure document workflows between EU and national institutions (Trusted Exchange Platform – e-Trustex), eSignature tools to support cross-border access to eServices for businesses, managing and supporting the exchange of information (GENIS – Generic Interoperable Notification Services), and Federated Authorisation Across European Public Administrations.

²⁹ On 9 April 2013, the second generation Schengen Information System (SIS II) with enhanced functionalities has entered into operation (e.g. the possibility to use biometrics, new types of alerts, the possibility to link different alerts and a facility for direct queries). SIS II consists of three components: a Central System, EU States' national systems and a communication infrastructure (network) between the Central and the national systems. Cf. the homepage http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm (last accessed: 31 March 2014).

European Network (CECIS); Europol (European Police), the European Union law enforcement agency that handles criminal intelligence; FIU.NET, the National Financial Intelligence Units exchange network for suspicious money transactions; and the FADO (False and Authentic Documents Online) network, a European Image Archiving System for exchange of information between Member States on genuine and false documents in the area of immigration and police cooperation.

INTERPOL maintains the secure I-24/7 global police communications system to connect law enforcement officers in the member countries. It operates “24 hours a day, 365 days a year”. Via this network, INTERPOL’s databases are accessible by authorised users (e.g. databases on suspected criminals or wanted persons, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of art). Police authorities can share sensitive and urgent police information with their counterparts.³⁰

I-link is considered by INTERPOL as the next level of data exchange. It is a unique and dynamic operational system that centralizes and continually enhances database features. I-Link provides an international structured communication standard, ensuring consistency and operational relevancy of recorded and exchanged police data. An important feature of the I-Link system is the direct recording of police information into INTERPOL’s criminal databases by the National Central Bureaus themselves instead of the General Secretariat.

3.2. Short overview of the knowledge repositories on the example of Austria

3.2.1. Public databases

E-Government databases and registries are in the basis for the information and communication infrastructure of the public administration. In recent years, the Austrian E-Government Strategy turned out to be an example of best practice.³¹ Besides offering many basic E-Government services on the Internet, electronic files, intelligent forms and an appropriate identity concept are milestones of efficient E-Government. Austria has very early deployed the electronic record system ELAK („Elektronischer Akt“), a document and workflow management system within the Austrian E-Government concept.³³ Further, Austria has a very well developed system of registers: Central Residents Register, Central Car Register, Commercial Register, Driving License Register, Identity Documents Register (Central Passport Evidence), Professional Register and Land Register.³⁴

The sector-specific personal identifier (ssPIN or bPk) is calculated using source PIN (Personal Identification Number, “Stammzahl”). and the naming of the one of the 26 sectors of E-Government. Thus, different identifiers exist for the various sectors. The cryptographic algorithm ensures that a bPk cannot be converted into another bPk. Thus, the concept of the bPk avoids the abuse of personal data as well as such “smart” use for security or law enforcement purposes.³⁶

Austria is one of the countries with a limited access of police/security services to public databases. Co-operation between authorities has to be based on administrative aid or crime prevention excluding direct access without a special authorisation.

³⁰ Cf. website: <http://www.interpol.int/INTERPOL-expertise/Data-exchange/I-link> (last accessed: 31 March 2014).

³¹ Cf. website: <http://www.digitales.oesterreich.gv.at/site/7908/default.aspx> (last accessed: 31 March 2014).

³³ Cf. website: <http://www.digitales.oesterreich.gv.at/site/6518/default.aspx> last accessed 9.2.2012.

³⁴ A. Winter, Zentrale Registerlösungen im föderalen Bundesstaat des 21. Jahrhunderts. In: Jusletter IT, 24. Februar 2011, http://jusletter-it.weblaw.ch/issues/2011/IRIS/article_300.html (2011).

³⁶ Cf. website: <http://www.stammzahlenregister.gv.at/site/5972/default.aspx> (last accessed 31 March 2014).

In the e-health sector, the “Main Association of the Social Insurance Organisations”³⁷ has established a central database containing administrative information regarding the existence of insurance, period of insurance, insurance contribution, the identity and address of the respective person and similar information. The access is subject to a special legal authorisation.³⁸ A much bigger index in e-health information is presently established, called ELGA.³⁹

Especially established for security purposes (which includes here also law enforcement purposes) is the Detection Services Evidence (this is an application that links two databases, the AFIS (= automated fingerprint-system) and DNA Database), Missing Objects Database, Car Tracing-/Information File, the Person Tracing File, the Arms Register, the Criminal Records and the Criminal Police File Index. The data sets mentioned above are interlinked by the system EKIS⁴⁵ (Elektronisches Kriminalpolizeiliches Informationssystem, Electronic Criminal Police Information System), which is an information compound system provided by the Minister of Interior for security and law enforcement authorities. The Federal Office for Constitution Protection and Counter Terrorism⁴⁶, which can be understood as the Austrian (internal) Intelligence Service, runs a data base called EDIS⁴⁷ which is – unlike EKIS – little known publicly.

3.2.2. Private Data Repositories and Applications

Private collections of data which can be interesting for security purposes could be detected in so many areas that it would go beyond the scope of this paper. In particular, data that are (free and publicly) available through the internet and – topically – in social media networks that are increasingly a source of interest for law enforcement services. Further, private CCTV has much more coverage as public CCTV. Special rules exist for data of particular interest for the fight against terrorism: Flight Passenger Name Records (PNR)⁴⁸, telecommunication data (“Data Retention Directive”⁴⁹), and financial transactions.

3.2.3. Financial Transactions

Tracking financial movements is a major tool to detect, prevent and/or prosecute crime in the financial system.⁵⁰ The regulation model that obliges financial institutions to keep their customers under surveillance, results in a two stage procedure. With other words, the financial institution first

³⁷ Hauptverband der Sozialversicherungsträger: <http://www.hauptverband.at> (last accessed 31 March 2014).

³⁸ For security authorities § 53 para. 3 Security Police Act (SPA), BGBl. (Federal Gazette) No.566/1991 as amended BGBl. (Federal Gazette) I No.33/2011; for law enforcement authorities § 89h Court Organisation Act, BGBl. (Federal Gazette) No.760/1996 as amended BGBl. (Federal Gazette) I No.136/2011.

³⁹ See the official information by the Federal Ministry of Health: http://www.bmg.gv.at/home/Schwerpunkte/E_Health_Elga/ (last accessed 31 March 2014).

⁴⁵ Cf. the website of the Austrian Ministry of the Interior: http://www.bmi.gv.at/cms/BMI_Datenschutz/ekis/start.aspx (last accessed 31 March 2014).

⁴⁶ Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT), http://www.bmi.gv.at/cms/bmi_verfassungsschutz (last accessed 31 March 2014).

⁴⁷ Electronically Data Information System (Elektronisches Dateninformationssystem).

⁴⁸ Cf. Commissioner Malmström: http://europa.eu/rapid/press-release_MEMO-12-259_de.htm (last accessed: 31 March 2014).

⁴⁹ Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union from 13.4.2006, L 105/54; now declared invalid by the European Court of Justice, case 293/12, Digital Rights Ireland, <http://curia.europa.eu> (last accessed: 31 March 2014).

This directive is under review due to heavy critics from civil rights organisations but also a request for a preliminary ruling by the Irish Supreme Court.

⁵⁰ Cf. Respect project, D8.1: Inventory of automated systems tracking financial movements used by private & public sector (2013).

determines whether a transaction is suspicious or atypical and notifies in a second step a state authority, the financial intelligence unit (FIU). Additionally, in some countries, there are certain thresholds which trigger automated notification of the FIU. The FIU analyses the received notifications and disseminates the results to law enforcement authorities, prosecutors or in the exercise of international cooperation to other FIUs.

Financial institutions monitor the transactions of their customers on the one hand to comply with international, European and national legal requirements and on the other hand to protect themselves for instance from reputational damage. Automated systems are deployed mainly in areas as anti-money laundering (AML), combating the financing of terrorism (CFT) and fraud detection. The major IT-solutions are used to conduct the Customer Due Diligence (CDD) procedure, to screen commercial watch lists and to monitor transactions.

The worldwide network for financial institutions enabling them to send and receive information about financial transactions in a secure, standardized and reliable environment is provided by The Society for Worldwide Interbank Financial Telecommunication (SWIFT) in La Hulpe, Belgium. This highly secure transport of financial messages is of particular interest for police/security services, in particular for the US-Terrorist Finance Tracking Program (TFTP). The “SWIFT-Agreement”⁵¹ between the USA and the EU gives the US-authorities direct access to this data subject to data protection guarantees.

To monitor customers’ transactions, financial institutions need to screen large amounts of data to evaluate whether suspicious transactions are being carried out. Atypical transactions generate alerts which invite employees to investigate these transactions. Legal provisions expressly require ensuring that transactions are consistent with the customer’s business and risk profile. Customers can either be profiled or assigned to a peer group, where deviations from the average behaviour of the group can be detected as suspicious.

Financial institutions have to examine whether their customers are on a watch list. Legal provisions stipulate how to interact with persons suspected to be involved in terrorism or money laundering and require enhanced monitoring of politically exposed persons (PEPs). Also, financial institutions are required to know about the beneficial owners of legal entities. Software vendors offer knowledge about beneficial owners, additionally some vendors carry out detailed background research on demand. Despite the use of highly sophisticated software, the final decision is generally taken by a human being and in case of exceptions, the decision is rapidly scrutinised and if necessary overruled by a human being.⁵²

3.2.3.1. GIANOS

An extraordinary product is the Italian GIANOS (Generator of Abnormality Indexes for Suspicious Transactions), produced by software vendor OASI Diagram-Outsourcing Applicativo e Sistemi Innovativi S.p.A., a company of the Banking Group Istituto Centrale delle Banche Popolari Italiane.⁵³ Approx. 99% of Italian banks are using GIANOS which was created by an inter-bank group, co-

⁵¹ Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Official Journal of the European Union L 195, 27.7.2010, p. 3.

⁵² Thomson Reuters Accelus, World-Check, IntegraScreen Reports. <https://www.world-check.com/de/our-services/integrascreen-reports> (n.d.). (last accessed 3 January 2014).

ordinated by the Italian Banks Association.⁵³ The Italian FIU is involved in determining GIANOS' algorithms and decision tables. As stated in a World Bank study this reduces pressure on financial institutions' employees trying to fulfil their reporting obligations.⁵⁵

3.2.3.2. Ma³tch Technology

The EU's financial intelligence units communicate with each other through the FIU.NET network, which deploys the Ma³tch technology to avoid the unnecessary exchange of sensitive personal data. The national FIUs store their respective data in their own databases. Relevant information for other FIU is represented in a vector, called a filter. This filter contains information about suspects converted into irreversible and therefore anonymised codes. Similar information is represented by similar filters that are shared between the FIUs. If data concerning an individual matches another filter, there will be a hit (hit/no-hit System). Then, FIUs can then decide whether it wants to request further information.⁵⁷ Filters created by the Ma³tch technology cannot be traced back to an individual.⁵⁴

1. Legal and technical constraints

Technology experts are aware of the misuse potential of smart exchange of data world-wide. Databases are considered as the hard core of the knowledge infrastructure. Therefore, access is always subject to sufficient trust between the services involved. Interfaces for a direct conjunction with other databases for data mining purposes are usually not provided. Having said this, it is not surprising that international data exchange systems are rather limited regarding their use of smart surveillance. Even though these systems have partly automated functions, the access interface is restricted to internal staff and secure e-mail technology, maybe intelligent forms. Cases of direct access are very few (e.g. in the framework of the Prüm Treaty) and subject to restrictions. The implementation of automated recording/logging routines shall ensure the traceability of information exchange and the lawful use of personal data. Privacy by design solutions like Ma³tch have been already developed.

The main constraints are legal, based on the human rights instruments, in particular the protection of privacy (Article 8 European Convention on Human Rights, Article 7 and Article 8 of the EU-Charter on Human Rights etc.). Therefore, the legal environment is now quite complex consisting of seven pillars of co-operation: INTERPOL, Europol, Schengen, Special international/European regimes (Prüm, VIS, EURODAC, PNR etc.), The Swedish Initiative (Council Framework Decision 2006/960/JHA), Council Framework Decision 2008/977/JHA, bilateral and multilateral agreements, and national law authorizations (allowing police forces to co-operate with other police forces if necessary). A new European framework has been proposed with the draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data.⁵⁶

This network can be considered as a very strong basis for data exchange between police authorities in Europe. Beyond Europe the cooperation is concentrated on the system of INTERPOL regarding the search of persons and objects. However, on this level the national law governing international co-operation and bilateral treaties are of higher importance since the scope of data exchange within the system of INTERPOL is more limited than within the European instruments.

⁵³ OASI, The GIANOS System and The GIANOS Procedure, Powerpoint (2005).

⁵⁴ #

⁵⁶ COM (2012) 10 final, 25.1.2012.

The most common safeguard mechanism is the so called “hit/no-hit” process⁵⁷. It consists of two steps: (1) A characteristic (e.g. fingerprint) is directly and automatically compared with the database. If a corresponding entry is found in the database, the requesting entity or person receives an identifier that cannot be assigned directly to a person. (2) With this identification, another request for the name and data of the matched person has to be applied for from a defined unit, e.g. the national Europol Contact Point. After a hit, e.g. according to the Treaty of Prüm, a request for such additional information (fingerprints, DNA profiles) has to be sent usually in the way like foreseen in the so called Swedish initiative.

Very good examples of “privacy by design” are the Ma³tch technology (see above) and a special access control system to the data collected under the Austrian data retention law (“Data Security Regulation”⁵⁸), the central “data hub”, the so-called “Durchlaufstelle” (DLS). Personal data are encrypted and exchanged between sender and receiver via the DLS. The DLS registers all transactions and generates statistics automatically.

4. Conclusions

The growing international data exchange, also between police/security services or financial intelligence units, is not surprising considering the globalisation of our life. With the rise of E-Government services, a European-wide or even international E-Government with extensive data exchange is coming. Technical constraints exist due to lack of interoperability but are more and more reduced. Common trust between involved services is still the major factor of co-operation and data exchange. Human rights standards constitute now the biggest restriction of data exchange. Police/security services have a quite complex system of legal authorisations and rules for data exchange at their disposal. The main problem are too many open textured clauses in more and more agreements, bearing the risk of too much sharing and no sufficient rules regarding the deletion of data. Advanced access regimes are best practice. The “hit/no-hit” process restricts access to information about existing data but not the content as such. The Ma³tch technology restricts data sharing to institutions having to deal with similar cases. Identification regimes with specific identities in the different sectors are also best practice (e.g. the system of Sector-specific Personal Identifier (bPk). It has to be seen if the proposed new Data Protection Regulation as well as the new Police/Security Services Data Protection Directive will improve the regulatory environment for data exchange.

5. Acknowledgements

This research was supported by the EU FP7 research projects SMART (contract no. 261727) and RESPECT (contract no. 285582). Websites: <http://smartsurveillance.eu/>, <http://respectproject.eu/>.

⁵⁷ SMART project, Deliverable D7.1.

⁵⁸ Datensicherheitsverordnung (TKG-DSVO), BGBl. (Federal Gazette) II Nr. 402/2011; the regulation is based on a study by the Ludwig Boltzmann Institute of Human Rights (BIM) on behalf of the Austrian Federal Ministry of Transport, Innovation and Technology (BMVIT). The final adoption contains some smaller amendments – which have to be criticised in the light of fundamental rights protection – but the substantial suggestions from the BIM have been transposed: <http://bim.lbg.ac.at/en/digital-rights/study-data-security-within-transposition-data-retention-directive-austria> (last accessed 7 February 2012).

CHALLENGES OF CONVERGENCE TO EUROPEAN MEDIA AND COMMUNICATIONS REGULATION – A MODEL FOR ANALYSIS

Hannu Nieminen

Professor of Media and Communications Policy, Department of Social Research,
Media and Communication Studies, University of Helsinki*
Expert in Public Service, the Administrative Council of the Administrative Council
of Finnish Broadcasting Company (Yle).
hannu.nieminen@helsinki.fi

Keywords: *Media and communications policy, media industry, public interest, media regulation, deregulation, re-regulation*

Abstract: *In the debates concerning media and communications policy, deregulation has been used as a synonym for liberalisation and privatisation. The assumption was that through deregulation media and communications industries would be liberated from the bureaucratic and ineffective state control to follow free competition. It was soon found, however, that in order to be effective and to provide the expected material benefits, the market still had to be regulated, and that some rules and restrictions were necessary. Simultaneously, it was realised that the media and communications differ from other industries in that their markets operate in the area of norms and ideas and that some normative rules are needed after all. Accordingly, media and communication policy in the last ten or so years has wrestled with the problem of how to balance these two different regulatory interests: the private interests of the industry, served by competition law, and the public interest, represented by the normative regulation. In this article, I develop tools for studying attempts to strike this balance by the use of different regulatory means.*

1. Introduction

In the debates concerning media and communications policy in the 1990s and early 2000s, one of the most commonly discussed concepts was deregulation. It was used as a synonym for concepts such as liberalisation and privatisation, meaning that the media and communications industries – specifically electronic media and telecommunications – were freed from the yoke of the state and its heavy-handed statutory regulation. Instead of serving politically defined normative ends with strict restrictions about competition and material gains, these industries were now supposedly liberated to follow free market ends and rules.

Or so it was thought then. However, it was soon found that in order to be effective and to provide the expected material benefits, the market still had to be regulated, and that, instead of unbridled free competition, some clear rules and restrictions were necessary. On the other

* Hannu Nieminen (hannu.nieminen@helsinki.fi) is professor of media and communications policy at the Department of Social Research, University of Helsinki, Finland. He received his Ph.D. in 1996 in the University of Westminster, London. His research interests include media and democracy, theories of public sphere, and communication policy and regulation. Currently he is leading a Finnish Academy funded project “Facing the Coordination Challenge: Problems, Policies, and Politics in Media and Communications Regulation” (2011-2015).

hand, it was simultaneously realised that the media and communications differ from other industries in that their markets operate in the area of norms and ideas and that some normative rules are needed after all. In stepped re-regulation.

Accordingly, media and communication policy in the last ten or so years has wrestled with the problem of how to balance these two different regulatory interests: the private interests of the industry, served by competition law, and the public interest, represented by the normative type of regulation. In this article, I develop tools for studying attempts to strike this balance by the use of different regulatory means.

2. Background

In the last 10-15 years, European regulation of media and communications has faced increasing challenges: the processes of globalisation and digitalisation have profoundly changed the media environment; consumer behaviour and media use are rapidly changing, punishing the print media and rewarding the mobile media; and European financial instability has rendered the future insecure.

The regulatory mechanism may be adapted to meet these challenges in a variety of ways. (See e.g. the discussion in Meier, 2011; also Black, 2002.) The traditional way of understanding regulation is government-centred, as a definition from the OECD makes clear:

Regulation is broadly defined as imposition of rules by government, backed by the use of penalties that are intended specifically to modify the economic behaviour of individuals and firms in the private sector. Various regulatory instruments or targets exist. Prices, output, rate of return (in the form of profits, margins or commissions), disclosure of information, standards and ownership ceilings are among those frequently used. (OECD, 2002.)

Lately, however, new regulatory needs and new actors have emerged, leaving this economy- and government-centred view wanting. The drive towards softer means of regulation in particular has brought new forms of self- and co-regulation to the fore. Summarising these changes, Julia Black has provided a critical definition of regulation:

[R]egulation is the sustained and focused attempt to alter the behaviour of others according to defined standards or purposes with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour-modification. (Black, 2002, p. 26.)

Black calls this a “decentred” concept of regulation: regulation is not restricted to the activity of government, nor is it based solely on legislation. Other sources may be used to justify it; it can be asserted by different actors; and regulators can apply different means for their own purposes. In what follows, I will discuss this decentred concept.

The division between concepts of regulation is reflected in differing notions concerning the societal goals of regulation. For what purposes is regulation needed? What are its goals and means? (Black, 2002, pp. 9-10.) Many researchers make a fundamental distinction between two regulatory ideologies, applied with different emphasis in the last decades: regulation for *economic efficiency* and regulation for *social and distributive concerns*. (Prosser, 2010, p. 4 and passim; see also Christensen, 2010.) According to Prosser, the first coincides with the concept of regulation as an intrusion on private autonomy; the second sees regulation as a collaborative enterprise (Prosser, 2010, pp. 4-5).

Traditionally, the regulation of the media (the press, electronic media) has followed the second ideology, serving public interest as defined in terms such as freedom of speech, public service broadcasting, pluralism of opinions and cultural diversity (Napoli, 2001; Harrison & Woods, 2007; Freedman, 2008; Meier, 2011; Lunt & Livingstone, 2012). In

contrast, the regulation of (tele)communications (including the Internet and mobile telephony) has mainly been based on the logic of economic efficiency (following the blueprints of competition policy). (See for example Bourreau, Cambini & Hoerning, 2011; EU, 2004.)

The aim of this paper is to critically explore recent conditions for democratic regulation of media and communications. It is assumed here that, for both technological and political reasons, the formerly distinct branches of the media and communications industries today intersect to the point where they are converging. It is assumed further that, whereas these branches used to be governed under different regulatory regimes (following the industry-specific approach) it now appears necessary to negotiate a new “converged” regulatory regime, balancing the diverging logics (towards a sectoral or multi-sectoral approach) (see Duijm, 2004).

3. Changes in the field

As mentioned above, media regulation has traditionally been guided by public interest principles that respect social and cultural aims. However, the regulatory landscape has changed almost beyond recognition in the last 25 years. In the late 1980s, the sectors of the media and communications were subject to industry-based regulation.

- **Print media:** Regulation is traditionally based on the freedom of the press principle (including goals such as pluralism and objectivity). There has been little statutory regulation, except for the ex-post¹ control of content based on criminal law and, in many countries, restrictions of ownership (Iosifidis, 2010).
- **Audiovisual media:** Most broadcasting in Europe used to be based on the principle of public service and state monopoly and couched in terms of specific legislation. In some countries (for example the UK and Finland), the commercial sector was regulated ex-ante by operating licences with content obligations, decreed by law.
- **Telecommunications:** In most European countries, telecommunications used to be a state monopoly operating under a Universal Service Obligation, guaranteeing basic telephony services to all households, supported by specific legislation.
- **Recorded media:** Regulation has been based mostly on copyright law (ex-post means), and implemented primarily by co- and self-regulatory means (through collecting societies).

Since then, the following fundamental changes have taken place (see Michalis, 2007; Harcourt, 2005; Charles, 2009; Hardy, 2008; Palez & Jakubowicz, 2003; Papathanassopoulos, 2002; Iosifidis, Steemers & Wheeler, 2005; Terzis, 2008; Terzis, 2007; Levy, 2001):

- Public monopolies (public service broadcasters, telecoms operators) have all but lost their status. Instead, the media landscape is increasingly characterised by the expansion of private companies and market fragmentation.
- Despite globalisation, there is no unified global regulatory framework for the media and communications market; the regulatory actors own conflicting competences (global, regional, national regulators; government agencies, co- and self-regulatory bodies, civil society watchdogs).

¹ Ex-ante means are “before the event” measures, which, in media and communications policy, include state subsidies and operating licences. Ex-post means are “after the event” measures, sanctioned, for example, in criminal and competition law

- As a result of technological convergence and digitalisation, content can be easily formatted for different markets. This has greatly challenged the basic legitimacy of traditional copyright regulation (controlling piracy and distribution of illegal content) and emphasising ex-ante regulation.

All these trends – globalisation, market fragmentation and technological convergence – have created a situation where traditional industry-based regulation has lost much if not all of its validity. The old regulatory framework struggles to balance the different interests represented in the field. This predicament is not, however, unique to media and communications regulation, but is shared within the wider field of regulation (see Prosser, 2010; Black, Lodge & Thatcher, 2005).

4. The regulator's viewpoint

In recent years, legislators have exerted great efforts to create an integrated regulatory framework for all media and communications. Some of the recent regulatory applications include:

- An attempt to attain technology neutrality in statutory regulation (Reed, 2007; MinTC, 2011);
- A drive for more concentration in regulatory surveillance and control (the establishment of independent regulatory authorities with a multi-sectoral approach) (EPRA, 2012);
- Soft law and co- and self-regulatory solutions, aiming for 'light touch' regulation;
- Emphasis on economic criteria as the main measure of regulatory efficiency (from ex-ante regulation to ex-post regulation).

This attempt to streamline media and communications regulation seems to distance it irreparably from its earlier social and cultural commitments and brings it closer to competition policy aims, measured solely by the criterion of economic efficiency. A major process is under way to renegotiate the concept of public interest that the media and communications are assumed to serve. If economic efficiency is seen as the goal, public interest is redefined in terms of unrestricted competition and "fair trade", which allegedly benefit both private firms, by equalising the terms of entry to the market, and the consumer, by lowering prices and offering better choice.

As the OECD puts it:

Different rationales for economic regulation have been put forward. One is to curb potential market power and increase efficiency or avoid duplication of facilities in cases of natural monopoly. Another is to protect consumers and maintain quality and other standards including ethical standards in the case of professional services provided by doctors, lawyers, etc. Regulations may also be enacted to prevent excessive competition and protect suppliers from unstable output and low price conditions, to promote employment and more equitable distribution of income. (OECD, 2002).²

In practice, this emphasis on economics is experienced in the way public service broadcasting has been dealt with in the EU. In the protocols to treaty of Amsterdam (1997), the duality of values concerning the media was clearly expressed: public funding of broadcasting was allowed only on the basis that it did "not affect trading conditions and competition in the Community to an extent which would be contrary to the common interest" (Amsterdam Treaty, 1997). This approach was further operationalised later in the

² Obviously, the two last aims – "to promote employment and more equitable distribution of income" – seem to sit rather uneasily with other rationales, as they cannot be measured by economic indices only.

2000s in the form of Public Value Tests (see Communication 2009/C.), in some cases opening the way for private media companies to intervene directly in the operational conditions of public service broadcasters (Donders & Moe, 2011; Lowe & Steemers, 2012).

5. An ideal–normative viewpoint

From a normative viewpoint, several researchers have claimed that the balance in media and communications regulation has tipped too much in favour of (private) economic interests (van Cuilenburg & McQuail, 2003; Meier, 2011). What should be done to correct this bias, and on what basis should a new balance be established? The following expresses one way to clarify the normative standpoint, from which a more qualified concept of public interest could be derived:³

In a democratic society, the media and communications system should serve citizens with all relevant information and orientation necessary for independent opinion formation and decision making. This includes that citizens are guaranteed, by statutory means if necessary, open access to all relevant information channels as well as equal availability of all relevant contents. Additionally, in order to promote public culture and to give citizens a voice, the media and communications system should offer citizens equal means for creative self-expression.

Using this definition as our normative guideline, we are left with the questions proposed above.

Regulation of what?

The regulation of the media and communications industries has traditionally differed from one sector to another. Can we assume that, because of technological and economic convergence, the increasingly intersecting sectors of media and communications can be governed and regulated as one entity? Or would a sector-based approach serve citizens' democratic needs better – and how can we define these sectors today?

Regulation for what?

In media and communications policy, the concept of public interest has traditionally been based on a balance between democratic societal needs and economic interests. In recent decades, this balance has shifted in favour of economic interests. The question is whether we should still aim to establish a “one-size-fits-all” definition of public interest in the new converged regulatory environment, the result of which might be that public interest is increasingly defined in terms of competition policy. Or would citizens' democratic needs be better served by the recent “hybrid” or multi-dimensional definition?

Regulation by whom?

In global media and communications policy, a five- to six-level regulatory system seems to be in development. This can be seen, for example, in the realm of copyright regulation: the global level (WIPO, 2012; TRIPS, 2012); the EU level (EU Copyright Directive 2001); national level (Finnish copyright act, 1961); co-regulatory level (Collecting Societies, 2012); industry self-regulatory level (e.g. attempts for DRM standardisation); and neo-corporatist (or joint-regulatory) level (Finnish Copyright Council, 2012). There is a problem of coordination, in that it is difficult or impossible to apply traditional concepts and modes of regulation to the new environment. This leads inevitably to confusion of competences and authority, even on the national level, as can be seen in the realm of Internet regulation.⁴ How

³ The following formulation is by the author.

⁴ There are several agencies in the field of Internet regulation with overlapping competences: Finnish Communications Regulatory Authority FICORE (network security), Consumer ombudsman (online services subscriptions),

democratic is this system? How is it coordinated? From the citizens' viewpoint, does it produce just and fair negotiating positions?

Regulation by what means?

Traditionally, the media have been regulated by a mix of ex-ante and ex-post means⁵, applied variably in different sectors of media and communications regulation, from state subsidies and television operating licences (ex-ante) to the control of advertising content and libel litigations (ex-post). Now, with the drive towards competition policy, ex-post means appear to be favoured exclusively. What would constitute the right combination? How should the indicators of economic efficiency be best reconciled with social and cultural aims?

6. An attempt to devise a model for monitoring regulatory development

How are we to pursue a critical analysis of the present regulatory regime? One way could be to assess how different regulatory means and instruments have affected public interest as defined above, by listing and analysing the different instruments applied in European media and communications regulation. This would offer a tool for long-term monitoring of European regulatory development.

Initially, we can identify several types of regulatory instruments, based on the following distinctions:

1. the distinction between
 - 1.1 ex-ante and
 - 1.2 ex-post regulation
2. the distinction between
 - 2.1 positive
 - 2.2 negative and
 - 2.3 neutral (if applicable) regulation
3. regulation by
 - 3.1 government
 - 3.2 co-regulatory bodies
 - 3.3 self-regulatory bodies
 - 3.4 a watchdog.

Below, I present an outline analytical table. In order to classify measures (positive ex-ante, positive ex-post, etc.), explicit criteria need to be created. By way of example, the classification could be conducted as follows:

- Positive ex-ante regulatory instruments include public service broadcasting (PSB) stipulations as well as operating licences for commercial television channels when conditions for content are stipulated.
- Negative ex-ante instruments include, for instance, public value tests, as they aim to limit the range of public service programming.
- Positive ex-post regulatory instruments are, for example, public rewards and prizes, granted to content providers for high quality.

Competition ombudsman (pricing of services, etc.),
Data protection ombudsman (privacy protection, etc.),
Police (protection of minors, etc.),
Save the Children (safer Internet),
Federation of the Brewing and Soft Drinks Industry (alcohol advertising),
The Copyright Information and Anti-Piracy Centre (CIAPC).

⁵ See the footnote 1.

- Negative ex-post instruments include penalty payments for operators violating licence conditions.

	Ex-ante measures	Ex-post measures
Positive means	<ul style="list-style-type: none"> • PSB stipulations • Broadcasting operating licences • Press subsidies • The MEDIA Programme • Market analysis & universal service obligation (USO) 	<ul style="list-style-type: none"> • Public rewards
Negative means	<ul style="list-style-type: none"> • Public value tests (public service broadcasting) • Audiovisual Media Services Directive (AVMSD) • Watershed stipulations (self-/co-regulation) • Alcohol advertising (statutory/self-regulation) • Ethical codes (self-regulation) • Ownership restrictions 	<ul style="list-style-type: none"> • Criminal law • Competition law • Ombudsman (statutory/self-regulation)
Neutral means	<ul style="list-style-type: none"> • Radio frequency auctions • Copyright law (statutory/co-/self-regulation) 	<ul style="list-style-type: none"> • Copyright enforcement (statutory/co-regulation)

Table 1: Categories of instruments applied in media and communications regulation

7. Concluding remarks

The basic assumption in this paper is that a shift has taken place in the regulation of the media and communications industries, favouring regulatory means formerly used mainly in the area of competition policy. By the same token, regulatory means based on democratic societal values have lost out. Simultaneously, however, there is growing awareness that, because of the wider societal and cultural value of the media and communications, regulation can no longer be based exclusively on economic goals. A new balance between democratic societal interest and economic need must be negotiated that does not disproportionately favour either side.

The continuing multilevel process of convergence makes it difficult to determine how best to coordinate the traditionally quite different regulatory systems of the media and communication industries. Not only do the sectors differ from one another, but also a wide array of regulatory instruments has been applied – sometimes for wholly dissimilar purposes. In this paper, an approach based on the distinction between ex-ante and ex-post regulatory means is discussed. It appears, at first sight, that democratic societal values have in the past been mostly served by positive ex-ante regulatory instruments, whereas economic interests have been promoted mainly by negative ex-post means.

Further analysis is needed to establish whether the proposed approach is fruitful in exploring the means for democratic regulation of the media and communications.

8. References:

Amsterdam Treaty (1997). 11997D/PRO/09: ‘Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts – Protocol annexed to the Treaty of the European Community – Protocol on the

system of public broadcasting in the Member States'. Official Journal C 340, 10/11/1997, p. 0109.

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:11997D/PRO/09:EN:HTML>.
(Retrieved 15 October 2012)

Black, J. (2002). 'Critical reflections on regulation'. *Australian Journal of Legal Philosophy*, 1(27), 1-35.

Black, J., Lodge, M., & Thatcher, M. (Eds.) (2005). *Regulatory innovation: A comparative analysis*. Cheltenham: Edward Elgar.

BIS (2011). 'The state aid guide: Guidance for state aid practitioners'. Department for Business, Innovation and Skills. June 2011. <http://www.bis.gov.uk/assets/biscore/business-law/docs/s/11-1040-state-aid-guide>. (Retrieved 15 October 2012)

Bourreau, M., Cambini, C., & Hoerning, S. (2012). 'Ex ante regulation and co-investment in the transition to next generation access'. *Telecommunications Policy* 26 (2012), 399-406; doi:10.1016/j.telpol.2011.11.024. (Retrieved 15 October 2012)

Charles, A. (2009). *Media in the enlarged Europe: Politics, policy and industry*. Bristol: Intellect.

Christensen, J. G. (2010). 'Public interest regulation reconsidered: from capture to credible commitment'. Paper presented at "Regulation in the Age of Crisis", ECPR Regulatory Governance Standing Group, 3rd Biennial Conference, University College, Dublin, June 17-19, 2010.

Collecting Societies (2012) 'Copyright organisations in Finland'.
http://www.minedu.fi/OPM/Tekijaenoikeus/oikeuksien_hallinnointi_ja_hankinta/?lang=en.
(Retrieved 15 October 2012)

Communication (2009) 'Communication from the Commission on the application of State aid rules to public service broadcasting'. (Text with EEA relevance) (2009/C 257/01.) Information from European Union Institutions and Bodies, Commission. 27.10.2009. Official Journal of the European Union C 257, 1-14. [http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009XC0930\(02\):EN:NOT](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009XC0930(02):EN:NOT).
(Retrieved 15 October 2012)

Donders, K., & Moe, H. (Eds.) (2011). *Exporting the public value test: The regulation of public broadcasters' new media services across Europe*. Gothenburg: Nordicom.

Duijm, B. (2004) 'On the institutional setting of ex-post regulation in regulated industries'. <http://www.garsonline.de/Downloads/Regulation%20of%20Airports/021108-Duijm.pdf>.
(Retrieved 15 October 2012)

EPRA (2012) 'European Platform of Regulatory Authorities'. <http://www.epra.org/>.
(Retrieved 15 October 2012)

EU Copyright Directive (2001) 'Copyright directive and related rights in the information society'.
http://europa.eu/legislation_summaries/information_society/data_protection/126053_en.htm.
(Retrieved 15 October 2012)

EU (2004) 'EU competition policy and the consumer'. Luxembourg: Office for Official Publications of the European Communities.
http://ec.europa.eu/competition/publications/consumer_en.pdf. (Retrieved 15 October 2012)

Finland Copyright Act (1961) 'Finland Copyright Legislation 2010. Unofficial Translations in English.' Ministry of Education and Culture

<http://www.finlex.fi/en/laki/kaannokset/1961/en19610404.pdf>. (Retrieved 15 October 2012)

Finnish Copyright Council (2012) 'Copyright Council.'

<http://www.minedu.fi/OPM/Tekijaenoikeus/tekijaenoikeusneuvosto/?lang=en>. (Retrieved 15 October 2012)

Freedman, D. (2008). *The politics of media policy*. Cambridge: Polity.

Harcourt, A. (2006). *European Union institutions and the regulation of media markets*. Manchester: Manchester University Press.

Hardy, J. (2008). *Western media systems*. London: Routledge.

Harrison, J., & Woods, L. (2007). *European broadcasting law and policy*. Cambridge: Cambridge University Press.

Iosifidis, P. (2010). 'Pluralism and concentration of media ownership: measurement issues.' *Javnost–The Public*, 17(3), 5-21.

Iosifidis, P., Steemers, J., & Wheeler, M. (2005). *European television industries*. London: BFI.

Levy, D. (2001). *Europe's digital revolution: Broadcasting regulation, the EU and the nation state*. London: Routledge.

Lowe, G. F., & Steemers, J. (Eds.) (2012). *Regaining the initiative for public service media: RIPE 2011*. Gothenburg: Nordicom.

Lunt, P., & Livingstone, S. (2012). *Media regulation: Governance and the interests of citizens and consumers*. London: Sage.

Meier, W. A. (2011). 'From media regulation to democratic media governance'. In Trappel, J., Meier, W. A., D'Haenens, L., Steemers, J., & Tomass, B. (Eds.) *Media in Europe today* (pp. 153-166). Bristol: Intellect.

Michalis, M. (2007). *Governing European communications: From unification to coordination*. Lanham, MD: Lexington.

MinTC (2011). 'Regulations for electronic communications to be gathered in one location'. Press release 06.09.2011. Ministry of Transport and Communications, Finland. <http://www.lvm.fi/web/en/pressreleases/-/view/1268461>. (Retrieved 15 October 2012)

Napoli, P. M. (2001). *Foundations of communications policy: Principles and process in the regulation of electronic media*. Cresskill, NJ: Hampton Press.

Nielsen, R. K. (2011). 'Public support for the media: A six-country overview of direct and indirect subsidies'. With Geert Linnebank. A Report. Oxford: Reuters Institute for the Study of Journalism.

http://reutersinstitute.politics.ox.ac.uk/fileadmin/documents/Publications/Working_Papers/Public_support_for_Media.pdf. (Retrieved 15 October 2012)

OECD (2002). 'Regulation'. In Glossary of statistical terms.

<http://stats.oecd.org/glossary/detail.asp?ID=3295>

Palez, D. L., & Jakubowicz, K. (Eds.) (2003). *Business as usual: Continuity and change in central and eastern Europe*. Cresskill, NJ: Hampton Press.

Papathanassopoulos, S. (2002). *European television in the digital age*. Cambridge: Polity.

Prosser, T. (2010). *The regulatory enterprise: Government, regulation and legitimacy*. Oxford: Oxford University Press.

Reed, C. (2007). 'Taking sides on technology neutrality'. In *Script-ed*. 4(3), September. <http://www.law.ed.ac.uk/ahrc/script-ed/vol4-3/reed.pdf>. (Retrieved 15 October 2012)

Springer, M. (2006). 'Considerations on DRM standards'.

http://camorra.org/drm_standards/. (Retrieved 15 October 2012)

van Cuilenburg, J., & McQuail, D. (2003). 'Media policy paradigm shifts: Towards a new communications policy paradigm'. *European Journal of Communication*, 18(2), 181-207.

Terzis, G. (Ed.) (2008). *European media governance: The Brussels dimension*. Bristol: Intellect.

Terzis, G. (Ed.) (2007). *European media governance: National and regional dimensions*. Bristol: Intellect.

TRIPS (2012). 'Trade-related Aspects of Intellectual Property Rights'.

http://www.wto.org/english/tratop_e/TRIPS_e/TRIPS_e.htm. (Retrieved 15 October 2012)

WIPO (2012). 'World Intellectual Property Organisation'.

<http://www.wipo.int/portal/index.html.en>. (Retrieved 15 October 2012)

EBOOK AND ACCESS RIGHTS

Anu Ojala

Researcher, University of Lapland, Faculty of Law
Yliopistonkatu 8, 96100, Rovaniemi, Finland
aojala@ulapland.fi

Keywords: *Basic right, copyright, contracting, contract, license, freedom of expression, freedom of communication, ubiquitous society, privacy, reader data, eBook, digital technology, end user, information infrastructure, ecosystem, publisher, writer, book, Apple, Amazon, Google, basic right, literature.*

Abstract: *When, looking at the impact of digital technology the ontology of our communication process's has changed; copyright law has not followed. Traditionally, copyright has at least somewhat tension relation with the freedom of expression and the complexities have only increased due to the digital technology. This development is obvious with eBooks and eBook contracting. At the digital era it is time to ask whether freedom of expression is enough and suitable to fulfill demands of democratic constitutional state.*

1. A World in the Making¹

1.1. Literature and Censorship

“Literature needs freedom and freedom needs literature.” This line is a citation from Guardian news,² where Burmese writer Ma Thida³ told about literature censorship in today's Burma. She concluded her speech by saying that “freedom and literature is mutually inter-related and cannot be separated from each other.”⁴ Even though at the first glance Burmese and Western censorship conflicting with the ability to write and read free seems different, at the end we return to the same basic questions; who has power and justification to decide the destiny of literature, and destiny of those people who creates, and those who reads it. Literature has been since ages an inseparable part of human history, and the old phrase “the pen is mightier than the sword” tells in one sentence those reasons why books have long history with censorship, and why we need to make sure that new threats against the freedom of the literature don't take over at the digital environment. Censorship at the digital age is a matter of relation between technology, copyright and contracts.

The nature of censorship has evaluated its character and it is not so obvious or simple as it has been understood to be at the time of the analogous world of communication. “Old fashioned” censorship is more masses of books on pure, flames eating the paper as in the Ray Bradbury's classic novel Fahrenheit 541, or just librarians who do not order those books on the library which they feel to be

¹ Title comes from Seipel's article. See FN 7.

² Thida, Literature needs freedom and freedom needs literature, the Guardian 2013

³ Ma Thida is a Burmese surgeon, writer and human rights activist. She was sentenced to prison for 20 years for “endangering public peace, having contact with illegal organisations, and distributing unlawful literature.” www.theguardian.com/profile/ma-thida

⁴ Thida, Censorship today, Keynote speech in Edinburgh World Writer's Conference 2013

harmful for the moral.⁵ Nowadays digital censorship is more hidden and more complex of its phenotypes, it is built inside the digital communication process the whole way through. That is why it is more powerful than earlier, and creates serious risks for cultural and communicational freedoms. Digital technology has given the censorship new layers to act, or in matter of fact, a new birth. As Seipel⁶ puts it, "Technology is never just technology. Technology is to be seen in its omnipresent cultural, social, and economic context. It is hardly ever "only a tool"." He concludes "...this is particularly essential in regard to artefacts which support and interact with our mental and bodily resources for information processing." He gives examples like alphabets, eyeglasses, books and typewriters.⁷ Nowadays we have more these artefacts connected namely to the information processing, or a communication process as used here, and more reasons to be aware of it due to the altered nature of this process from static form to the dynamic.

1.2. Theoretical Model to Handle Network Society and Information Infrastructure

By building a theoretical model (see p. 3) is described the relation between type of the society and the mode of modernisation when communication process is in question. The first level of the model defines the type of the society. We already live in the network society, our information infrastructure consists of growing amount of digital technology connected and converged to communication in its different forms. Wireless technology is one of the most important factors speeding up the development. Information infrastructure is at the model divided into traditional communication infra of analogical world, and digital communication infra. The newer part of the infrastructure, digital communication infra, and its development will have a profound effect what kind of mode of modernisation we will live within the network society. Basic factor is the access to the infrastructure; by what kind of terms access to the infrastructure and that technology which builds it is formed. At the recent years ubitechnology, namely ubiquitous computing,^{8, 9} has merged within our net society's information infrastructure. Saarenpää¹⁰ writes about the ubiquitous computing that if taking too far, new technology and new infrastructure both create temptations, and in concerto used and regulated could lead, and already had resulted in a development which piece by piece leads from the open society to the surveillance society, also called a naked society.¹¹ At this moment it has come clear that governments and companies way to use this technology for surveillance is so impudent that after Edward Snowden's disclosures¹² on digital surveillance

⁵ Finnish book censorship see for example Ekholm Kai: *Kielletyt kirjat 1944-1946*, doctoral thesis University of Oulu 2000. In other Ekholm's book *Kirjastot ovat palaessaankin kauniita*, tells how books have disappeared or destroyed for the political reasons. In the Soviet Union books and descripts were hidden at the glass bottles in a garden, in Tibet collectors destroyed books during Chinese Cultural Revolution, in Finland Yrjö Leino's *Ministerin muistelmät* was collected away even from bookshops and homes, p. 35. See also Syväla Maarit, Dammert Lauri, *Näitä ei tänne hankita! Kirjastojen aineistoja valvovat näkymättömät portinvartijat*, Suomen Kuvalehti 33/2012.

⁶ Professor Emeritus Peter Seipel is a founder of IRI (Stockholm University the Swedish Law and Informatics Research Institute). IRI was established in 1968 making it one of the oldest institutes in the field in the world. Seipel wrote his thesis "Computing Law Perspectives in New Legal Discipline" already 1977.

⁷ Seipel, *Copyright and a World in the Making*, p 1.

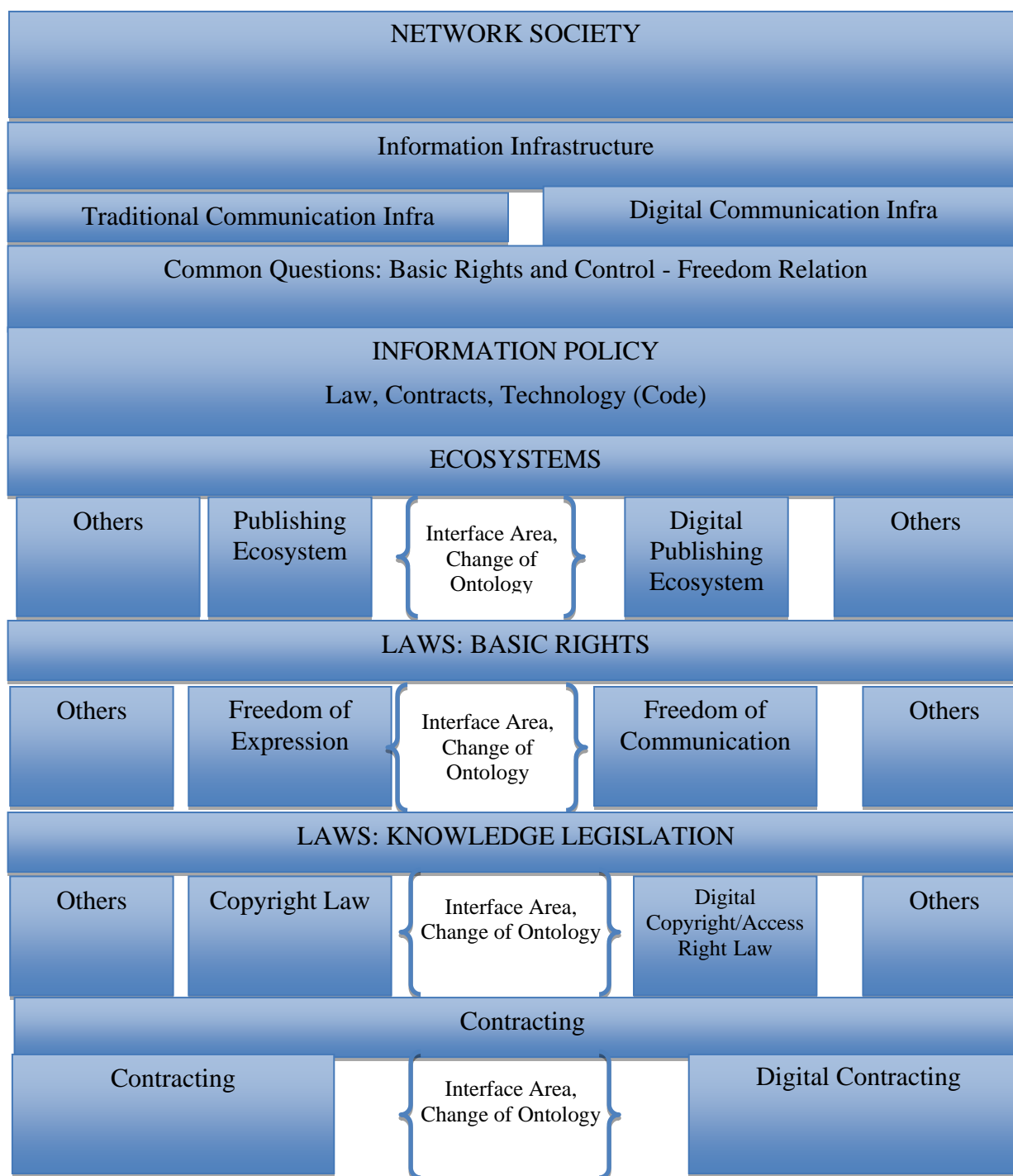
⁸ Mark Weiser was a chief scientist at Xerox PARC in the United States, and the first to write about ubiquitous computing. See memorial for Mark Weiser www-sul.stanford.edu/weiser. One of his writing is *The Computer for the 21st Century* at www.ubiq.com/hypertext/weiser/SciAmDraft3.html.

⁹ Terms artificial intelligence and everywhere are also used. See for example European Coordinating Committee for Artificial Intelligence www.eccai.org, Adam Greenfield: *Everyware: the Dawning Age of Ubiquitous Computing* 2006.

¹⁰ Ahti Saarenpää is professor of Private Law, Director of Institute for Law and Informatics (University of Lapland) and Deputy Chair of Data Protection Board.

¹¹ Saarenpää, *Oikeusinformatiikka*, 2012 p. 442

¹² See latest news on Snowden www.theguardian.com/world/edward-snowden?uni=Article:in%20body%20link



practised by the United States, the reality has been compared to George Orwell's famous dystopian novel Nineteen Eighty-Four¹³ and many similarities have been found.¹⁴

Society's mode of modernisation is dependent on the answers and solutions defining the status of the basic rights and the relation between control and freedom. Citizen's capability to be part of the communication process is essential for the right to self-determination. It is undeniable part of the

¹³ One consequence was that Orwell's 1984 book sales soared 6,000 %, see for example Osborne Hannah, George Orwell's 1984 Book Sales Soar 6,000 % on Edward Snowden NSA Prism Data Leak, International Business Times 11.7.2013 www.ibtimes.co.uk

¹⁴ Different issues is then is the future more Orwellian or than Huxley Aldous's novel The Brave New World, where is no need to hide the truth about society or right to information is not taken away from citizens, cause people just don't care. This might be more frightening dystopia, and somehow Snowden's statement that media has been more interested in his girlfriend than those disclosures he made, is symptomatic.

democracy and depends on the changing nature of mode of modernisation. One important issue part of the information policy is would it be possible or necessary to specify what way general legislation by using relating legislative techniques could take under consideration the digital market and profits it yields.

1.3. Digital Publishing Ecosystem

Second level of the infrastructure at the model are the ecosystems, which at the same time are extremely self-supporting, but on the other hand, depending on everything that happens to surround them. Through these ecosystems it is possible to mirror for example different legislation, regulations and contracts inside the ecosystem, and do comparison between different ecosystems to find out the inner relations, and weight of individual ecosystem at the wholeness of infrastructure.

As with the infrastructure in general, the question of access is substantial part of the ecosystems. eBooks and eReaders are the main factors of the digital publishing ecosystem, and one lock are the gatekeepers which are able to control functioning of the ecosystem, the cause of the so called silo effects. That is the consequence of the tethering nature of digital eBook technology. Risk of concentration in digital publishing industry is an issue to be estimated. Communication markets are not mentioned at model independently as such, they are formulated inside ecosystem being one way or another connected with public domain, either destroying it or giving space to flourish. This depends on for example what way copyright law and contracts handle the public domain.

Both publishing and digital publishing ecosystems will have a new face when this, at least somewhat painful transition reaches its saturation point. Many legacy publishers have problems to cope with the change and the new gatekeepers have not been hesitant to fully exploit the opportunity. Most of the new comers are tech firms, with background at devices and apps, and in addition to that, they know the Internet as a sphere of operations more than well. Harkaway describes this process writing "So Amazon, Google and Apple are gatekeepers. They have realised that the key to profitability is not investing in risky start-ups, but owning the marketplace where those start-ups stand and (mostly) fall."¹⁵ This shift to digital book markets and shift from pBooks to eBooks have been the fastest at the United States, but we here in Europe are following. At the same speed as citizens start to use eBooks and eReaders, the transformation is inevitable.¹⁶ Ubiquitous contracting and surveillance are now the major challenge headed in the world of the written word.

¹⁵ Harkaway, Amazon aren't destroying publishing, but reshaping it, 2012.

¹⁶ At the United States, according to Book Industry Study Group's survey Consumer Attitudes Toward E-Book Reading, eBook byers continue to shift from dedicated eReaders to tablets. The Study also shows the consistent upward swing in preference for e-books over print. About 82 percent of Power Buyers (consumers who acquire e-books on a weekly basis) say they prefer e-books over print and nearly 70 percent of Non-Power Buyers say they now prefer e-over print. Press release 5.4.2013 www.bisg.org. E-book is now fully embedded in the format infrastructure of Trade book Publishing. E-books grew 45% since 2011 and now constitute 20% of the Trade market, playing an integral role in 2012 Trade revenue. The most pivotal driver of e-books remains Adult Fiction, with Children's/Young Adult also showing strong numbers. Press release 15.3.2013, Bookstats Volume 3: Publishing the most comprehensive annual survey, www.bisg.org In Finland development in general by publishing for tablet platform has been fast. In 2010, number publications of this kind was none eBooks, newspaper nor magazines. Next year 2011 numbers were growing: 1300 eBooks, 10 newspapers and over 20 magazines, 2013 about statistics showed 2500 eBooks, over 20 newspapers and plenty look-a-like papers, over 100 magazines and look-a-like magazine applications. Viestinnän keskusliitto: näkökulmia sähkökirjoihin ja kirjastoihin, Markkula Kristiina, Suomen Kustannusyhdistys, VKL, Virva Nousiainen-Hiiri, Helsingin kaupunginkirjasto-yleisten kirjastojen keskuskirjasto 2013. In Finland publications in general the net selling price, exclusive of VAT (1 000 €) was 245 529 , amount of digital publications was 17 425. <http://tilastointi.kustantajat.fi> Digital publications were counted also audiobooks and online-publications.

1.4. Basic Rights

The third layer of the model is the basic rights. In digital communication environment it is time to evaluate the freedom of expression, created for the need of analogical information infra, able to manage the demands of digital communication process. Core issue is thus the ontology of the freedom of expression fit into digital publishing ecosystem cause of the changed nature of the whole communication process related to the reading of books. Besides the access-problematic, also privacy matter is connected to eBooks, both performing the role in the fulfilment of freedom of expression.

There is a relation between right to read anonymously, reader data, privacy and freedom of expression. This is the result of the technological tools which makes possible to control and track purchase and use of eBook. Characteristic of eBook technology is problematic and it creates risks for democracy. Privacy's role alongside the freedom of expression has stronger position than earlier and issue of the reader privacy has to be solved. As the United States Supreme Court already at 1953 stated "Once the government can demand of a publisher the names of the purchasers of his publications, the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of anyone who reads. The purchase of a book or pamphlet today may result in subpoena tomorrow. Fear of criticisms goes with every person into the bookstall... Some will fear to read what is unpopular, what the powers-to-be dislike... If the Lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries, bookstores, and homes of the land. Through the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press."¹⁷

According to Saarenpää "Principles of information law are desperately needed in the new network society. The leading principles are (1) the right to know, (2) the right to information, (3) the right to communication, (4) freedom of information, (5) the free flow of information, (6) the informational right to self-determination and (7) the right to information security; at least those."¹⁸ When analysing the ontology of the freedom of expression, the principles of information law should be used in that evaluation to see what the flaws are when digital communication process is in question.

Saarenpää continues "It is important to understand that they (information law principles) are meta-fundamental rights at the level of social contract. Then we have other, implementing principles at the level of written fundamental law. Interoperability should find its place there too."¹⁹ This is important to take into account cause the requirement of interoperability would solve some problems with eBook and eReaders as tethering technology. Tethering has its own part to do with the freedom of expression issues.

It is questionable whether the freedom of expression is able to answer these new problems and challenges in the digital world. We might have need to create a new basic right, the freedom of communication to handle the special features of digital communication process, like access and privacy issues more detailed.

¹⁷ United States v. Rumely, 345 U.S. 41, 57, 58 (1953) (Douglas J. concurring)

¹⁸ Saarenpää here continues that "The leading principles are (1) the right to know, (2) the right to information, (3) the right to communication, (4) freedom of information, (5) the free flow of information, (6) the informational right to self-determination and (7) the right to information security; at least those. Saarenpää, Interoperability and Legal Interoperability 2013 p. 5.

¹⁹ Saarenpää here continues that "The leading principles are (1) the right to know, (2) the right to information, (3) the right to communication, (4) freedom of information, (5) the free flow of information, (6) the informational right to self-determination and (7) the right to information security; at least those. Saarenpää, Interoperability and Legal Interoperability 2013 p. 5.

1.5. Knowledge Legislation

Fourth level of digital information infrastructure is knowledge legislation. It is important to be aware of as Litman puts it that “What is crucial, though, is that we recognize that our intellectual property laws form the basic legal infrastructure for our information policy in an online world.”²⁰ At the Digital publishing ecosystem and eBooks in question, copyright law is one of the most important laws.

Books have a long history with copyright. The Statute Anne emergence as Gutenberg created new technology, the printing press. Books faced with the developed technology and copying and distribution came to a problem specifically for the publishers. The new exclusive rights in a form of privileges saw the light. That was 1600 century’s technology war, which still has strong impacts on today’s copyright system. Somewhat odd ways, the same happens now again, and we are heading toward of our own time digital technology war zone. Digitalization and convergence are responsible for their own part that authors and publishers are once again, after quite calm 300 hundred year period, looking worried in the future and wait what is happening.

Scope of the copyright protection widened after DRMs were installed inside copyright law and given regulative shelter. Already at the early days of DRMs Ginsburg noticed that “Even if an “access right” does not precisely correspond to either of the traditional copyright rights of reproduction or public performance, it does respond to what is becoming the dominant way in which works are in fact exploited in the digital environment.”²¹ Heide handled also same problematic by writing “In the Web environment access is fundamental. To be sure, just like the hard-copy world every act of experiencing or using works of authorship involves an act of access. The Web, however, allows the seamless combining of the ability to control access with the ability to control uses in the hands of the same entity.”²² With eBooks also the control of technology might be under the same companies as the control of access and use of the work.

DRMs installed inside copyright law with consequences. As Still writes “The legal protection of DRM systems affects the inner logic of copyright. As the copyright system is a dynamic whole, a change in one part of the system provokes a reaction (or a series of reactions) in other parts of the system.”²³ Still continues on access issues that “The application of DRM systems may increase the power of copyright holders to govern the use of the copyrighted work, the question arises whether DRM systems actually provide new rights for copyright holders, not only improved the possibilities of enforcing existing rights.” Still describes how the legal discourse has been “a heated debate on whether DRM systems actually provide a new right to control access to the work even after first publication.”²⁴

Use of the contracts supported by technology gave rise to a new kind of private ordering. Elkin-Koren and Salzberger write this problematic and have concluded that “DRMs possess the ability to turn information, once a non-excludable resource, into a more excludable asset and exceed the time span of excludability long after purchase by consumers and, indeed long after the expiration of IPR granted by legislation. This fundamental change transforms not only the nature of informational works but also relationship between the right holders and consumers of copyrighted material.”²⁵ With the help of DRM -technology and contracts content neutral e-book technology might turn to a contend/user -based censorship tool. After this alteration has the issues of access to the works, control and restrictions of the use of the work, and collecting reader data opened the door for the

²⁰ Litman, *Copyright New Paradigms*, p. 8.

²¹ Ginsburg, *From having copies to Experiencing Works*, 2000 p. 8.

²² Heide: *Copyright in the EU and U.S.: What “Access-Right”?* 2001 p. 10.

²³ Still, *DRM och upphovsrättens obalans* 2007 p. 341.

²⁴ Still, *DRM och upphovsrättens obalans* 2007 p. 333.

²⁵ Elkin-Koren, Salzberger, *The Law and Economics of Intellectual Property in the Digital age*, 2013 p. 219.

reader's contractual and privacy problems. Because of the massive use of DRMs connected with contracts, copyright as a regulative tool is not the same as it used to be.

Other problematic to mention is the question what work category eBook belongs to, cause it might contain many work categories like text, drawings, music, animations, also interactive versions, games, photographs, cinematographic works, maps, computer programs, databases etc. There are more often both copyright and related rights in question, eBook is not always just an electronic version of the printed book and in the future this will be more usual.²⁶ Blurring lines of the work categories cause problems as for example exemption-system differs for work category basis. Access right might answer better for the needs of the fluid works; works in digital format with dynamic nature and acting in dynamic communication process where the status and environment of the work is easily altered.

Access right is the key issue also with copyright, cause digitality creates situations and problems of a kind which traditional copyright is not able to solve. Database right for example might be used a wrong way. At the first evaluation of the database directive were written that "the issue of access to "information" is of concern for various categories of users as it may involve information in the public domain; information where the database constitutes the only available source of that information, information pertaining to academic and scientific research and...",²⁷ list continues there. So, there is a reason for that as Borghi and Karapapa write "...The sui generis database regime potentially creates an entitlement over content, which may be either in the public domain or not eligible for copyright protection –such as raw scientific data or information and metadata on content. ... The sui generis database right provides a powerful extra layer of protection where copyright does not apply."²⁸ Having books also in digital format and gathered under big collections we might face this problem in concreto if right holders choose to build up for example certain kind of monopoly and keep protection layers as strong as possible.

1.6. Digital Contracting

The Fifth step of the model is contracting, which in digital form could be described being ubiquitous. Moving inside digital publishing ecosystem, there are contracts in their different forms everywhere you click your way.

Contract-dilemma could be divided three main classes when eBooks in question; contracts between writers and publishers, contracts between publishers and intermediates, and end user contracts.²⁹ Every chain of contract has impact on issue of access, use and control of eBook. One main challenge for example is that the traditional copyright law is not able to cope the contractual issues between writers and publishers when eBook in question. That has started to lead collecting of rights from writers for perpetual time, and for the future technologies. This is one factor media concentration development. Author's central role in digital publishing ecosystem should be seen also in copyright law. Writer Margaret Atwood used the title "The Publishing Pie: An Authors View" when she was speaking about the relationship between digitality and writers. She reminded in a colourful way that writer is a primary source in cultural food chain comparing that when a

²⁶ See for example Baddley: Sutler by Richard House –review in guardian. News is about first enhanced thriller. www.theguardian.com/books/2013/mar/24/sutler-richard-house-review

²⁷ Commission of the European Communities, First evaluation of Directive 96/9/EC on the legal protection of databases, p. 9.

²⁸ Borghi, Karapapa, Copyright and Mass Digitization, 2013 p. 100.

²⁹ The whole contracting chain is wider if starting from those basic needs like access to the internet, devices, software, hardware, and access to the webstores, needed to purchase and use eBook.

moose dies, it feeds over 3 dozen other species and the same way author and author's book sustains many other life forms.³⁰

With end user contract, one fundamental question is that traditionally when buying a book, you own that copy and copyright remains for the right holder. Now, when buying an eBook, the purchaser cannot be sure what she/he has bought. Maybe all that is transferred is a license to use eBook under strict scrutiny, and only with good luck, question is about a sale, and reader has a digital copy of eBook, which is his or hers alone. This difference between a license and a sale is crucial as: what you do not own, you cannot control either. This is a question of the judicial definitions of purchase, and the problem of publishers or intermediaries ability to control the access and use of the eBook the rest of its existence after it has been purchased. Other main issue here is that citizens contract away their basic rights, right to privacy and copyright's freedom of expression's guarantees.³¹

Problems of contracting at the digital publishing ecosystem are from the scientific journals points of view researched by Willinsky, and result of his work shows some problems. In his book about open access to research and scholarship Willinsky defines problematic of digital age, that even we have technical capabilities to spread information wider than ever before, the movement of concentration is strong in the scientific journals and result as the diminishing amount of papers at the universities libraries. Willinsky writes "This age-of-information paradox follows on the successful transformation of knowledge into a capitalized commodity and economic driver. ... The resulting corporate publishing concentration, with its relentless focus on knowledge capitalization and shareholder value, has seen journal prices increase well above inflation rates, and university libraries cannot keep up. ... The publishing goal is not necessarily increased circulation of journals."³² He has faced the problem now seen in publishing business in general, that the end result of the digitality might be something else than was expected.

One kind of the contractual problem is caused by the nature of eBook itself. eBook is much more complicated to be managed than its printed counterpart. There are questions of cumulative rights and relations with the right holders, and classification of work. eBooks is not just a book anymore. Al Gore's eBook "The Choice" for example can be purchased on Apple's Appstore not the iBookStore, and that matters cause the end user terms are different.³³ By whom is it defined what is a book and what an application? Al Gore's blog's headline is "Our choice App Launch Today",³⁴ even many other instances Our Choice is understood as eBook.³⁵

As the ending words here it could be cited what Goldstein and Hugenholtz wrote: "Access and use of the infrastructure and access and use of the content demands citizens to agree with agreements. Contract law has rapidly become a regular companion to copyright protection as the structure of the Internet enables the formation of contract relationships between information producers and end users, either directly or through intermediaries."³⁶ It is a serious problem for the democracy if private contracting is this kind of way taking place from the public laws.

³⁰ Heikkilä, TOC Tools of Change of Publishing, p. 23.

³¹ Traditionally, copyright's freedom of expression guaranties are idea/expression dichotomy, exceptions-system and limited term of copyright. Use of these guaranties is dependent on access to the work.

³² Willinsky, The Access Principle, 2009 p. 17. John Willinsky is professor at Stanford Graduate School of Education, and a developer of Open Journals Systems software.

³³ www.apple.com/legal/internet-services/itunes/bw/terms.html

³⁴ Gore, Blog: Our Choice App Launch Today, 2011

³⁵ See for example Lee, Al Gore's "Our Choice" App Reinvents Books, Reading. At the headline Our choiced is labeled as a App, but at the story says "...the startup has created an ebook that talks, spins, moves, and folds, featuring video, interactive infographics, maps and more, all seamlessly interwoven with the text in a way that helps bring the concepts to life. Huffingtonpost.com/2011/04/28/al-gore-our-choice-app-push-pop-press_n_854783.html.

³⁶ Goldstein, Hugenholtz, International Copyright, 2013 p. 345.

2. Some Thoughts at the End

At all levels of the digital information infrastructure, starting point is always access, the core heart of the freedom of communication. Denial of access to the infra at some stage the most likely would make impossible to move to the next level. For example, if you do not have Internet connection, you are not able to get into an eBook store at the web, or if you do not have any kind of reader device or software, you are not able to order or read eBook. One of the most central access-dilemmas is copyright law because knowledge legislation affects the whole communication process.

Other big problem from the freedom of communication point of view is that there is a track left after every use of the infra, and that way a reader privacy problem is activated. We do not have clear enough legislation, or even political will at European Union nor in the United States, as Snowden case has shown, to have strict rules, or follow the rules if exist, what way user data is used and privacy respected. Freedom of communication should have a structure guaranteeing the right to govern user information, at minimum we need to know what all is collected and where, when it is used and why, and is somebody getting some benefits from it. Right to own personal information should be taken more seriously, only owner should be able to give consent for example to sell this information.

Reader Data is sensitive information, it is political data and it should be under strict rules how it is handled so that privacy of readers is not jeopardized. The knowledge that somebody, private business and/or government is able to track what you are reading, might cause silent censorship. Beside active censorship, also this self-censorship is dangerous if taken too far.

There are questions where we need to have answers. Is it legally binding or even reasonable to contract away copyright's freedom of speech guaranties and privacy rights? What way today's twisted contractual situation will affect writers and the kind of literature they write? Do we truly have a right to read under surveillance? At the core there is how many private gatekeepers should have informational powers in their hand, and what might be the societal risk for that we want to accept. We will see are we heading towards ethical mission impossible: digital publishing ecosystem with the balanced digital copyright law and the respect of the basic rights.

On ACLU's Issue Paper on Digital books, it is said why freedom to read in privacy matters: "What you choose to read says a lot about who you are, what you value, and what you believe. That's why you should be able to learn about anything from politics to health without worrying that someone is looking over your shoulder."³⁷ The same is true also for the writers, they need freedom to breathe and write. Democracy needs sharp pens and brave voices making questions, so we can stay in tune with the way the society is developing. Digital copyright's master task is to guarantee balanced communication process where ontology of law confronts with reality, and enables balanced digital environment for the writers, publishers and readers. Even in the world of ones and zeros literature comes from the true heart and need honest writing free from censorship any kind. That is important because "Art is not a mirror to reflect reality, but a hammer with which to shape it" as Bertolt Brecht would say.

3. References

ACLU of Northern California. Digital Books: A New Chapter for Reader Privacy. www.aclunc.org/issues/technology/digital_books_a_new_chapter_for_reader_privacy.shtml

Apple, The terms of use [www.apple.com/legal/internet services/itunes/bw/terms.html](http://www.apple.com/legal/internet-services/itunes/bw/terms.html)

³⁷ ACLU of Northern California. Digital Books: A New Chapter for Reader Privacy.

Borghi Maurizio, Karapapa Stravroula. Copyright and Mass Digitization, Oxford University Press 2013

Elkin-Koren Niva, Salzberger Eli M. The Law and Economics of Intellectual Property in the Digital Age. Routledge Research in Intellectual Property (2013)

Efroni Zohar, Access-Right. The Future of Digital Copyright Law. Oxford University Press 2011

Commission of the European Communities, DG Internal Market and Services Working Paper, First evaluation of Directive 96/9/EC on the legal protection of databases, Brussels, 12 December 2005

Ekholm Kai, Kirjastot ovat palaessaankin kauniita, BTJ Kustannus 2010

Ginsburg Jane C., From having copies to Experiencing Works: the Development of an Access Right in U.S. Copyright Law, Columbia Law School, Public Law & Legal Theory Working Paper Group, Paper Number 8, 2000

Goldstein Paul, Hugenholtz Bernt, International Copyright. Principles, Law and Practice. Oxford University Press 2013

Gore Al, Our Choice App Launch Today, [bloghttp://blog.algore.com/2011/04/our_choice_app_launch_today.html](http://blog.algore.com/2011/04/our_choice_app_launch_today.html)

Harkaway Nick, Amazon aren't destroying publishing, but reshaping it, 26.4.2012 <http://m.guardian.co.uk/books/ebooks+cat=books>

Heide Thomas: Copyright in the EU and U.S.: What "Access-Right"? Journal of the Copyright Society of the USA, Vol. 48, No. 3, Spring 2001

Heikkilä Harri, TOC Tools of Change Publishing. Matkaraportti ja ajatuksia uudesta julkaisemisesta. 14-16.2.2011 New York, Next media projekti, Aalto-yliopisto

Lee Amy, Al Gore's "Our Choice" App Reinvents Books, Reading, www.huffingtonpost.com 28.4.2011

Litman Jessica: Copyright New Paradigms in Growing Pains 63 (1997) eds. Laura A. Gassaway

Saarenpää Ahti, Interoperability and Legal Interoperability –Tensions between Technological, Linguistic and Legal Points of View, 2013

Saarenpää Ahti, Oikeusinformatiikka, in Oikeusjärjestys, 8. Painos, Lapin yliopiston oikeustieteellisiä julkaisuja Sarja C 59, University of Lapland 2012

Saarenpää Ahti, Perspectives on Privacy on Legal Privacy eds. Ahti Saarenpää LEFIS 2008

Seipel Peter, Copyright and A World in the Making, ALAI World Views Paper

Still Viveca, DRM och upphovsrättens obalans, IPR University Center Publications 2007

Thida Ma, Censorship today, Keynote address at Edinburgh World Writers'Conference www.edinburghworldwritersconference.org/censorship-today/thida-in-malaysia-keynote-on-censorship-today/ 23.6.2013

Thida Ma, Literature needs freedom –and freedom needs literature, shorter version from Censorship today at www.theguardian.com/books/2013/jun/24/literature-freedom-burma-ma-thida 24.6.2013

Willinsky, John, The Access Principle. The Case for Open Access to Research and Scholarship. First MIT Press paperback edition (2009)

Cases

Supreme Court of the United States: United States v. Rumley, 345 U.S. 41 (1953).

COPYRIGHT AND THE DIGITAL ENVIRONMENT

Niklas Bruun

IPR University Center
Hanken School of Economics, Finland
niklas.bruun@iprinfo.com

Keywords: *Copyright, digitalization, enforcement, legitimacy of copyright, media convergence*

Abstract: *The digital revolution has brought into daylight a number of problems for the traditional legal regulation of copyright. The article explores different problem areas and also discusses solutions.*

1. Introduction

Technological development since the 1990s, with the Internet and digitalization, has been a revolution where the Internet has changed our communication patterns and daily life over a short period of time. The kind of typewriter that I used for writing my doctoral thesis some years ago, has been passed to history so effectively that when a representative of a younger generation encounters such an object from the 1980s today, he can be heard saying: “Dad, what a strange computer”. On the other hand, development has taken place successively and gradually: It was only several years after the Internet's breakthrough that music could be distributed via the network on a larger scale, and it is only recently that the web has become an efficient and common distribution channel for films and other audiovisual productions.

The debate over digitalization and copyright has now been going on for nearly two decades. Opinions differ and the issue is contentious. I myself think that we have now reached the point where it is possible to get an overview of the problem, and that it is perfectly feasible to do a sort of closing of the books regarding what has happened, where we stand today and which kinds of solutions we should seek to the problems that we face. The purpose of this presentation is to try to present a brief overview of the issue.

What is clear already, is that copyright in particular, but also intellectual property law in general, has become a central branch of law in our new information or network society. After all, the fundamental aspect of modern technology, namely computer programs, or software, is protected by copyright. Everyone who uses a computer bases his activity on licenses that include the right to use copyrighted software. The problem with copyright in the digital environment is that copyright has become overloaded with functions and expectations.

The basic function of copyright is still there: It is expected to reward creativity and financially incentivise innovation. This has been accomplished through various commercial stakeholders, such as publishers, record companies, media companies etc. that guarantee continuous compensation to the author, whenever his work or production is used for a financial benefit. The author has an interest in controlling how his creative work is being used in different contexts, and in receiving compensation for various uses. This compensation, for what is usually called creative content production, must also be guaranteed in the digital environment. Legislation must provide a framework that allows the author to exercise his rights both individually and collectively.

New technology also provides authors with unprecedented opportunities to directly reach out to consumers: creation, distribution, dialogue and communication (also through networks).

In any case, the digital environment also brings about a number of problems, which are still partly unresolved, and which undoubtedly require that copyright and different behavioural patterns or business models are adjusted or changed in various ways. In what follows, I will consider and describe seven key problem areas or aspects, where the adaptation of copyright to the digital environment must be gradually implemented, and where we currently have a number of tensions between new technology and traditional control that has been developed over a long period of time.

These problem areas, which are of course partly intimately connected, can at first be listed as:

1. Media convergence problems
2. Copyright law as a barrier or brake on, firstly, new business models and services for citizens, and secondly, on the activity and innovation of citizens
3. The tension between copyright and the technological possibilities of making a huge heritage of literature, film and other audiovisual works, as well as various databases, available to the public
4. The transformation problem in copyright law, or the problems related to the use of legal concepts from an analogue world in a digital environment
5. Copyright law and the tension between national and international regulations and markets
6. The enforcement problem and the problems related to monitoring copyright, and finally
7. The legitimacy problem in copyright law.

2. Problem Areas

2.1. Media Convergence

It is often argued that copyright law is media neutral or technology neutral. It shall apply equally regardless of how and in what form, or what kind of technology the author used to make his work available to the public. In the analogue world it was relatively easy to create media-specific compensation systems and rights to control the use of protected works. Typical examples are photocopies or private music-recordings. By introducing targeted compensation systems for different uses we have been able to compensate authors for the private use of their works, for example by introducing copying fees or by charging a specified fee for empty cassettes. Today, different methods for using these media have become integrated, you can store music on your computer and mobile phone, and you can store enormous amounts of content on new storage platforms. All this has made the question of how to develop a traditional compensation system for private use of copyrighted material extremely complicated. This has led to lengthy debates and disputes about how the compensation systems should be developed.¹

2.2. Copyright Law as a Barrier to New Business Models and Services for Citizens

Some prominent economists and business strategists view copyright law as an obstacle and a barrier to the emerging digital economy. Especially companies engaged in making the works of other people available to the public, for example Google providing databases or search engines, often perceive strong copyright protection as an impeding factor in the progress of the digital world.

It is not difficult to find examples of how copyright issues can slow down the emergence of new services. One question we dealt with within the Copyright Council, which I had the honour of chair-

¹ See e.g. on Finnish discussion Wessberg, Aarne, Hyvitysmaksujärjestelmän vaihtoehtoinen järjestely, Opetus- ja kulttuuriministeriön selvityksiä 2011:21. Helsinki 2011.

ing, was the availability of so-called network PVR services.² PVR stands for the English term Personal Video Recorder, and as we all know, it has long been possible for everyone to save their favourite shows on their digital decoders and then watch them later. This activity is personal private copying. Now, new technology facilitates different types of services, which can offer an on-line selection of missed or previously broadcasted television programs to prospective customers. The option of watching different TV-programs whenever you want and without regard to the official program is popular among consumers, and Yle, as well as other service providers, have made such services available, for example Yle-Areena. Needless to say, it is technically possible to offer such advanced services, while it is problematic to clarify rights and create an effective contractual system.

Another international example of a form of service, which is at least partially prevented due to copyright issues, is Google's project to digitalize the world's literature. Google scanned more than 10 million books under an agreement with more than 30 major libraries. The intention was to make literature available to consumers via the Internet. Many of the books that were scanned were, and are still, protected by copyright, and so The Authors Guild in the United States brought an action against Google for copyright infringement. The trial, which was conducted in the form of a class action, i.e. the idea was to resolve the problems also with regard to authors who did not participate in the process, became widely known and is still going on. The result is that Google has been prevented from building the kind of extensive selection of literature that it had hoped for.³ – It is clear that in the prospect of future e-books, it would be a huge step forward for us all if different forms of literature could be available online. The question is of course whether libraries and public cultural institutions should undertake this task, or whether a private company should be able to acquire a monopoly in this area.

The digitalization of our film heritage is also an important issue. Within the IPR University Center at the University of Helsinki we have recently cooperated in a study for the European Commission, about the preservation of the European cultural heritage with regard to films.⁴ The background here is, as we all well know, the fact that in the digital world you don't need film to photograph your family on a holiday trip, nor do you need film to produce a movie. There has been a significant technological change in the production of movies: For example, only 2% of the movie production in Great Britain in 2004 was so-called born-digital, while 70% of the production was done digitally in 2009. At the same time cinemas are also becoming digital, so that analogue film projection will cease in commercial cinemas within the European market within the next few years. This will have drastic consequences for old analogue movies; if you want to preserve them and make it possible to show them to an audience, they must be digitalized. Digitalization is expensive and many European countries lack even the kind of film archives that Finland has, where national films are preserved. The problem of digitalization is also that it is difficult to get private stakeholders to participate, because it can be difficult to sort out who has copyright to these movies in order to be able to exploit them commercially. The question regarding how digital movies can be preserved is also important, as we know, technology is constantly being developed and archiving requires active measures. – In other words, the digital environment makes it technically possible to create an outstanding film archive from around the world, and to make it available on-line for each one of us. However, at present it is still unclear how this will turn out, there is an obvious risk that much of our film heritage will be lost in this digital transformation.

² See Tekijänoikeustoimikunnan mietintö – Ratkaisuja digiajan haasteisiin (Solutions to the challenges of the digital age). Opetus- kulttuuriministeriö. Työryhmämuistioita ja selvityksiä OKM 2012:2. Helsinki 2012.

³ See more Bruun, Niklas, The Google Book Search Battle – a Global Issue, IPR Info 2/2010.

⁴ See Bruun, Niklas, Is Copyright an Obstacle? Preserving Audiovisual Heritage, IPR Info 2/2011. 17–18. See also the report "Challenges of the Digital Era for Film Heritage Institutions", http://ec.europa.eu/avpolicy/docs/library/studies/heritage/final_report_en.pdf.

2.3. The Role of Copyright for the Activity and Innovation by Citizens

In the digital environment works are often created through the use of earlier works created by others. The new technology makes it easy to copy and paste pictures, music and other material into works created by individuals for a non-commercial purpose. In an analogue environment, this could take the form of private use; in a digital environment blogging or making works available online means that the works are being made available in a way that requires the author's permission. In practice, this often leads to uses that are contradictory to copyright law, but which are of such little financial significance that no action is taken against them. The discussion regarding this kind of User Created Content, and whether or not it should be allowed under special regulations, has been addressed by, among others, the European Commission.⁵ Furthermore, social media has led to the boundaries between private and public becoming extremely complex or even erased.

The digital environment has made the application of copyright law extremely complicated in schools and universities. The traditional mind-set of making exceptions for the use of material protected by copyright, for the benefit of research and teaching, has been somewhat reduced. A good example is the restrictions on what can be shown in education: Under special agreements teachers are allowed to make tape recordings or to record television programs and show them in class. But within copyright law a Youtube video is in principle an audiovisual work or a film, which requires a special permission in order to show it in class legally, although implicit consent to such a use can probably be assumed in some cases.

This development has had clear counter reactions in the form of new types of copyright clauses that emphasizes openness: *Open Source*, *Creative Commons* and *Open Access*. These are also based on copyright law, but they create opportunities for a more generous use of works, and a creative development of what others have achieved. In the new digital environment these types of contractual arrangements should be used more systematically within schools, universities and public administration. The problem has been the difficulty of combining openness with the traditional exclusive rights based on copyright law, and the lack of a systematic effort to develop a new type of culture, based on a kind of hybrid between openness and free use, in combination with exclusive intellectual property rights. That is what I believe will be needed in the future.

2.4. The Transformation Problem in Copyright Law

Within legal science, one important debate over the principles relating to copyright in the digital environment, has stated the question whether the fundamental concepts and principles in copyright law can, as such, be applied in a digital environment, or whether they would need to be revised. In other words, the question is whether the terminology of copyright law be transferred or transformed as such to the new environment? My view is that the basic concepts need to be revised in the new media reality of today. The starting point for today's regulations is that it is the public conveying of works to the public (making them available) that should be protected by copyright. This conveying has traditionally been considered to occur in two ways: either through the production and distribution of copies or directly through a performance to an audience present at the performance. The problem in the digital world is that the difference between the production of copies and the direct conveying becomes more or less fictional or even misleading, because the question whether or not production of copies occurs de facto may in individual cases depend on technical circumstances. Nevertheless, the communication of works by wire or by wireless means has been introduced as a separate category in order to cover the digital conveying of works. However, I'm inclined to agree with Professor Ole-Andreas Rognstad from Norway, who suggested that the exclusive rights of

⁵ See Copyright in the Knowledge Economy. Communication from the Commission 19.10.2009. COM (2009) 532 final p. 9.

rights holders in the digital world should be redefined to include the fair use of a work or presentation.⁶ In this way one could avoid the nomenclature leading to a pointless discussion of whether the production of a copy has taken place in a variety of more or less relevant circumstances in the digital environment. Such legal development would provide a good opportunity to extend copyright protection to certain relevant uses, which today seem to be unclear, while excessive protection could be denied in situations where rights holders' control over the work seems unreasonable. Clearly this is not uncontroversial, but it would make the discussion and argumentation focus on the relevant questions.

2.5. Copyright Law as a Barrier to Internationalization

Within the European Union it is often stressed that the Internet has no national borders, but that the markets for online services is divided and fragmented within the EU. The European Commission believes that it is necessary to create a governance regime for a European copyright system in order to manage the relationships between authors, commercial users and consumers in a good way in Europe. It is certainly true that some stakeholders have this problem, if for example Nokia wants to offer music services on their mobile phones, they must at present purchase separate licenses in every European state, and the copyright organizations they negotiate with will generally have only a national mandate. On the other hand, there are many markets that are still distinctly national; Finnish-language literature or popular music that is sung in Finnish, will probably have limited demand in Europe. So the question is how to simultaneously create better conditions for cross-border solutions, without causing problems for the national stakeholders and contractual systems that are in use.

2.6. The Enforcement Problem in Copyright Law

Copyright in the digital environment cannot be discussed without going into the question of realization of rights in practice. This is one of the major questions, which has been on the agenda ever since the 1990s. Exceedingly, two questions have been in focus: one concerning various technological measures to protect works as well as the legal protection of works.⁷ The other question relates to the role and responsibility of network operators in situations where the copyright holder, for various reasons, finds it difficult to take action against the copyright infringer.

As for technological measures to protect works, they are now regulated in copyright law and are now a part of the tools that the copyright holder can use to protect his rights. Technological measures to protect works have been used primarily in e-commerce, whereas in the consumer goods industry consumers have tended to abandon products that have been protected by different restrictions on use.

The question of the responsibility of network operators is one of the most controversial in the digital copyright. Within the EU it was resolved at one point by the approval of the E-Commerce Directive, which protected operators from financial responsibility for illegal material on the net, as well as from an obligation to oversee or monitor the content that is transferred in the networks they provide. Network operators have often been compared to telephone companies or the postal service providers. What happens on the telephone lines or in enclosed letters does not concern the provider of the telephone line or the postal service.

⁶ See Rognstad, Ole-Andreas, *Opphavsrettens innhold i en multimedieverden - Om tradisjonelle opphavsrettsbegreper møte med digital teknologi*. NIR 2009. 531–547.

⁷ See Still, Viveca, *DRM och upphovsrättens obalans*, IPR University Center 2, Helsinki 2007.

The exception to the freedom enjoyed by network operators is the so called "notice and take down" procedure, which means that when there is illegal material on the Internet, and network operators are informed about this, they must remove the offending material.⁸

In recent times there have been trials in different countries, including Finland, where rights holders have demanded the right to block access to IP addresses that exclusively or predominantly provide infringing material.⁹ Legislation to that effect has been introduced or planned in several countries.

The Copyright Council also proposed that such legislation should be introduced in Finland.¹⁰ Our proposal is based on an application process in which a court could order a telecommunication services provider to prevent its customers from accessing an Internet address/homepage that aims to make material protected by copyright available to the public, without permission from the rights holder. The requirement for such prevention is proposed to be, in addition to the network address being known, that the prevention cannot be considered unreasonable with regard to the rights of the person making the material available to the public, or with regard to the rights of intermediaries or authors.

This proposal has been met with sharp criticism from network operators. Also other stakeholders, such as the Pirate Party and a number of writers on cultural matters have been critical towards the proposal.¹¹ It is therefore important to stress that we now have a situation where IP addresses are being registered overseas in countries like Turkey and Armenia. These addresses can be completely focused on the Finnish market, for example showing Finnish movies, without any compensation paid to the authors or rights holders. Now we are also starting to see the faces of these actors, and they are by no means so called young nerds or students who share music or movies with their friends. We have seen pictures of Kim Dotcom, the boss of the website MegaUpload, who allegedly is of Finnish origin and has earned 150 million euros with his network service, most of which is based on the business idea that you should not pay copyright remuneration.

It is true that blocking access to a network address is not a particularly effective weapon, as the business can quickly be relocated to a new address or be accessed via some other route. Even so, research has shown that many consumers give up when the address is blocked, and that it takes time to make a new address known and popular among users.

In my mind, it is surprising that a proposal based on the idea that a network address that is intended to distribute material that is protected by copyright is blocked by a specific court decision, where all interests and circumstances are considered, is still described as censorship of the web and something that is impossible to realize. What is less surprising is that network operators or the so-called independent organizations financed by them, such as EFFI¹², stand critical to the proposals, they make good profits when online activity flourishes.

The starting point is of course that we should protect the neutrality of the web, and that we should be extremely cautious when requiring operators to take action against unsympathetic or offensive content. And the principle that network operators should not be allowed to oversee the contents of network communications is a cornerstone for all digital communication. On the other hand, the transnational nature of the web cannot lead to the immunity of organized crime, which chooses to

⁸ See 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 178/1. 17.7.2000.

⁹ See Helsinki District Court case 26.10.2011, Music Producers IFPI and others. v. Elisa Oyj. Decision 11/41552, where Elisa was ordered to block some of Pirate Bay's Internet addresses.

¹⁰ See OKM 2012:2 p. 35–69.

¹¹ See e.g. Esa Mäkinen in Helsingin Sanomat 27.1.2012.

¹² See www.ffi.fi.

operate from a country where the basic principles of a society based on the rule of law cannot be upheld and realized.

2.7. The Legitimacy of Copyright Law

The discussion on copyright in the digital environment is definitely not complete if the question of the legitimacy of copyright law is not addressed. Copyright has been heavily criticized in the digital environment, partly because of the shortcomings that I have already discussed, but also partly because the answer, from the point of view of the rights holders, to the challenges of the digital environment, has often been a one-sided emphasis on the need to strengthen the exclusive right; to extend it to new areas such as databases or program concepts, to extend the length of the protection period and to create more severe sanctions for violations of rights. Lawrence Lessig has described this as the desire to maintain the Read/only culture of the 1900s, which maintains a view of copyright as protected from rewriting and linked to tangible storage media, while the Read/Write culture of the digital environment is not allowed to develop.¹³

Stefan Larsson has recently defended his thesis "Metaphors and Norms. Understanding Copyright Law in a Digital Society" at the University of Lund.¹⁴ He argues that there is now a fundamental conflict between the social norms that characterize the digital environment and the legal norms emanating from the copyright system. And he believes that there is path dependence from the traditional copyright regulations, which tends to colonize the protection of consumers and the neutrality of Internet service providers.

3. Final Words

The paradox is that copyright has become increasingly important while it has become increasingly controversial. The digital environment cannot survive without copyright; it is needed and is an essential foundation of the Information Society. But it is clear that we cannot keep on trying to maintain out-dated business models with the help of a strict copyright, instead, the digital environment requires new solutions for many stakeholders. However, we cannot create a digital environment where it is perfectly legal for new participants to use material produced by others – without permission – in order to get further momentum for their own business models. Obviously, those who provide search engines and databases are tempted by such a strategy. A wise societal copyright strategy must carefully avoid these extremes¹⁵, while the tremendous opportunities for cultural interaction in the digital environment should be utilized much better than today.

4. References

Bruun, Niklas, The Google Book Search Battle – a Global Issue, IPR Info 2/2010.

Bruun, Niklas, Is Copyright an Obstacle? Preserving Audiovisual Heritage, IPR Info 2/2011. 17–18.

"Challenges of the Digital Era for Film Heritage Institutions", European Commission Report http://ec.europa.eu/avpolicy/docs/library/studies/heritage/final_report_en.pdf.

Copyright in the Knowledge Economy. Communication from the Commission 19.10.2009. COM (2009) 532 final.

¹³ See Lessig, Lawrence, *Remix: making art and commerce thrive in the hybrid economy*. New York; London: Penguin Press 2008.

¹⁴ See Larsson, Stefan, *Metaphors and Norms. Understanding Copyright Law in a Digital Society*. Lund Studies in Sociology of Law 36. Lund University. Lund 2011.

¹⁵ For a detailed argument, see van Eecke, Patrick, *Online service providers and liability: A plea for a balanced approach*. Common Market Law Review (CMLR) 48: 1455–1502. 2011.

- Eecke, Patrick, Online service providers and liability: A plea for a balanced approach. *Common Market Law Review* (CMLR) 48: 1455–1502. 2011
- Larsson, Stefan, *Metaphors and Norms. Understanding Copyright Law in a Digital Society*. Lund Studies in Sociology of Law 36. Lund University. Lund 2011
- Lessig, Lawrence, *Remix: making art and commerce thrive in the hybrid economy*. New York; London: Penguin Press 2008.
- Rognstad, Ole-Andreas, Opphavsrettens innhold i en multimedieverden - Om tradisjonelle opphavsrettsbegrepers møte med digital teknologi. *NIR* 2009. 531–547.
- Still, Viveca, *DRM och upphovsrättens obalans*, IPR University Center 2, Helsinki 2007.
- Tekijänoikeustoimikunnan mietintö (Report of the Copyright Commission) – Ratkaisuja digiajan haasteisiin (Solutions to the challenges of the digital age). Opetus- kulttuuriministeriö. Työryhmämuistioita ja selvityksiä OKM 2012:2. Helsinki 2012.
- Wessberg, Aarne, Hyvitysmaksujärjestelmän vaihtoehtoinen järjestely, Opetus- ja kulttuuriministeriön selvityksiä 2011:21. Helsinki 2011

PRIVACY FRIENDLY REMEDIES FOR INTELLECTUAL PROPERTY RIGHTS

Mindaugas Kiskis

Professor, Mykolas Romeris University, Communication and Informatics Institute
Ateities g. 20, Vilnius LT-08303, Lithuania
mkiskis@mruni.eu; <http://www.mruni.eu>; <http://www.kiskis.eu>

Keywords: *Data protection, privacy, intellectual property rights, remedies, enforcement*

Abstract: *The paper analysis the privacy challenges of enforcing intellectual property rights on the internet. Existing remedies are generally incompatible with user privacy, hence they place additional burden on the enforcement of rights, and unnecessary opposition between the fundamental rights of privacy and the intellectual property rights. Existing regulations and case law, emphasizing these challenges, are reviewed. The paper also investigates enforcement of trademark rights online as a successful example of aligning privacy and enforcement interests. Domain seizure and takeover through the existing UDRP system is successful and is generally a privacy friendly remedy, dealing with trademark rights infringement in domain names. The author suggests that expansion of the extra-judicial domain seizure through UDRP to broader use of intellectual property enforcement may be a useful privacy-friendly addition to the existing remedies, and would allow certain marginalization of intellectual property rights infringements online.*

1. Introduction

Advanced data transfer technologies caused major expansion of the infringement of intellectual property rights on the internet. Under pressure from the intellectual property rights holders, the governments around the world responded mainly through increased enforcement efforts, attempts to introduce new substantive legal rules governing illicit online activities, as well as attempting large scale prosecutions of internet users downloading and sharing content files on the internet.

In Europe attempts to establish a new substantive framework for enforcing intellectual property online were made at the regional level initially in the Council of Europe Cybercrime Convention of 2001, later in the EU Enforcement Directive 2004/48/EC, and most recently in the Anti-Counterfeiting Trade Agreement of 2011. At the national level additional initiatives through the “three strike” approach or other impact to the infringing internet users were enacted. The practical result of these efforts was filtering and blocking of various internet resources, disconnection of the users from the internet, as well as all sorts of traditional sanctions and civil remedies (damage awards, confiscations of infringement instruments (computer equipment), etc.). In many cases the results were ineffective and even counterproductive, since they have caused public outrage, raised awareness of intrusions into individual activities online and public concerns about disproportionality of intellectual property rights remedies.

The purpose of this paper is to explore the privacy challenges of the traditional remedies, when they are implemented online, as well as privacy challenges caused by the new “three strikes” and internet filtering remedies. Regulations and case law pertaining to these problems are reviewed and analyzed. The paper also investigates enforcement of trademark rights online as a successful example

of aligning privacy and enforcement interests. Domain seizure/takeover through the existing UDRP system is a successful privacy friendly remedy dealing with trademark rights infringement in domain names. Based on the analysis, the author suggests that expansion of the domain seizure through UDRP to broader use of intellectual property enforcement may be the needed privacy-friendly addition to the existing remedies. Comparative, cartesian, empirical and epistemic methods of analysis are employed for the analysis in the paper.

2. Legal context for collisions of privacy and intellectual property rights enforcement

Privacy in the EU is well established and fundamental rights are extensively regulated. Principal rules for protection of privacy in the EU are set forth in Directive 95/46/EC, which is in the process of being replaced by the European General Data Protection Regulation sometime in 2014 or later. Privacy in the electronic communications is additionally regulated in Directive 2002/58/EC.

For the purposes of the enforcement of intellectual property rights and application of remedies, it is most relevant that personal data under Directive 95/46/EC (i.e., national rules implementing this Directive) can only be processed for specified explicit and legitimate purposes, for a period of time established in advance and may not be processed further in a way incompatible with those purposes (Art. 6 b). Data may be processed only under the legitimate processing criteria (Art. 7). Express rights for the data subject are also established, and shall be communicated to him or her prior to processing of personal data.

In case of infringement of intellectual property rights by the individual, processing of his or her data in order to respond to the infringement is unavoidable. When the processing is done for the purposes of enforcing the public law, such processing is generally admissible and justified according to the said data protection legal framework, however when private law enforcement is sought none of the principal legitimate processing criteria (such as an unambiguous public interest, consent or a contract) are clearly present. Processing of individual's personal data in such situations (such as collecting sufficient evidence that particular individual has infringed intellectual property rights) at best can rely on the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject. This criterion is the vaguest of all data processing criteria. It also makes the data collecting party entirely liable for the proper interpretation of the situation. If the interests for fundamental rights and freedoms of the data subject (the individual who infringed the intellectual property rights) are found to be more important, it means that the data was collected and controlled illegitimately, thus, making it inadmissible as evidence and potentially exposing the data controller to liability for improper processing of personal data.

Just a suspicion that the individual infringed the intellectual property rights may not be sufficient for legitimate processing of his data by a private party. Moreover, significant incriminating evidence may be necessary in order to pierce the privacy of the internet user, who is identified only indirectly – by IP address, avatar or nickname. Note that requesting and imposing judicial remedies against the individual infringer is in many cases impossible without precise data on the identity of the individual. Online users' identities are almost always represented through indirect personal data (such as the IP or e-mail address), which is not fit and sufficient for judicial applications, i.e., IP or e-mail address cannot be indicated in a lawsuit in place of the physical address. Differently from the USA, most European countries do not allow lawsuits against anonymous defendants (so called Jon Doe lawsuits), and even in the USA the complexities of litigating against anonymous defendants

(essentially a separate legal case in order to identify the individual user) have led to the demise of this approach¹.

Further data protection rules that are problematic from the point of view of IPR enforcement are data subjects rights. The data subject has the rights to know about the processing and to access all data processed about him or her, that is – evidence, which may be incriminating for the infringement of IPR (even for civil law enforcement). The data subject even has the right to demand the rectification, deletion or blocking of data that is incomplete, inaccurate or isn't being processed in compliance with the data protection rules (Art. 12 of the Directive 95/46/EC).

Personal data may be processed only insofar as it is adequate, relevant and not excessive in relation to the purposes for which such data is collected and processed. The data must be accurate. The data controller shall ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified. The data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected (Art. 6 the Directive 95/46/EC).

All of the above are reiterated in the draft European General Data Protection Regulation and make the job of collecting evidence (which is almost indiscriminately personal data) by private parties (and especially by individual IPR holders), subject to strict regulatory restraints. Even the simple identification of infringers on the internet becomes a legal problem due to complex privacy and data protection requirements discussed above. This conflict between privacy and intellectual property enforcement interests is not new and has become evident immediately during first attempts to enforce intellectual property rights online more than a decade ago².

These legal problems have been deliberated in almost all European jurisdictions, and despite the accumulating case law remain open. According to the ECJ case law in C-275/06 *Promusicae v. Telefonica* case, privacy rights are recognised as fundamental human rights, which can be restricted only in exceptional cases, expressly set forth in the laws and strictly following the proportionality principles. It is further set forth in the *Promusicae* case, the protection of intellectual property must be balanced against the protection of fundamental rights of individuals which would be affected. The ECJ did not establish the exact requirements for when online users' privacy can be pierced (his identity disclosed based on IP address)³, however established that it cannot be discretionary.

The *Promusicae* case was generally interpreted as requiring significant proof and vesting this burden of proof on the right's holder, who is alleging infringement of the intellectual property rights. In order to access and disclose the personal data needed to initiate legal proceedings, the suspicions of infringement are not sufficient. Body of evidence, which unambiguously and consistently supports the case of infringement, may be necessary in order to compromise the privacy of the suspected infringer of intellectual property rights. It is important to recall that online service providers (along with any information society service providers) according to the provisions of the EU Electronic Commerce Directive 2000/31/EC (Art. 15) have no general obligation to monitor or otherwise process (gather and store) information on the activities of their clients online, including data, which would identify a specific user as the initiator or participant of a specific activity online. This specifically includes absence of the general obligation to actively to seek facts or circumstances indicating

¹ Bridy, Annemarie, Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement. Oregon Law Review, Vol. 89: 81, 2010, http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1698542_code630766.pdf?abstractid=1565038&mirid=1 last accessed on 15.03.2013 (2010)

² Richardson, Megan, Downloading Music off the Internet: Copyright and Privacy in Conflict? Journal of Law and Information Science, Vol. 13, No. 1, p. 90-106 (2002).

³ Coudert, Fanny; Werkers Evi, In The Aftermath of the Promusicae Case: How to Strike the Balance? Int J Law Info Tech 18 (1): 50-71 (2010).

illegal activity. The only general exception is when such data and identifiers are necessary for the business practices and accounting of the intermediary. Another group of exceptions is set forth in the EU Data Retention Directive 2006/24/EC, however neither of these exceptional cases is applicable to the infringements of intellectual property rights online.

Said approach, disallowing discretionary exceptions from privacy rules, has been adopted in national legal doctrines in several European countries, among them in the Lithuanian constitutional doctrine even before *Promusicae* (September 19, 2002 resolution of the Lithuanian Constitutional Court in the case No. 34/2000-28/01). In some countries (e.g., the Netherlands) some online services providers have adopted full anonymity of the users as their business model. They expressly declare that no information, which can identify the individual user behind the IP address or another electronic identifier, will be collected, processed, stored or made available. In these cases it may be impossible to connect the indirect electronic identifiers (such as the IP address, which may be issued randomly) to the specific individual user. Concerns over privacy violations have led to the emergence of the alternatives to judicial remedies, such as the “three strikes” analysed below.

On the remedies side the principal legal framework is established in the EU through Directive 2004/48/EC, which to date remains the principal supranational legal framework in the EU, which provides main remedies against infringement of intellectual property rights online. National law has generally relied on these rules (or in some countries preceded) therefore is not analyzed separately.

Directive 2004/48/EC requires from all EU Member States to apply equal, efficient, effective and proportional sanctions and remedies against the infringers of intellectual property rights, especially in cases, when intellectual property rights are infringed on a commercial scale. Directive 2004/48/EC primarily focuses on the counterfeiting of trademarks, as well as infringements of patent rights, however regulations pertaining to the copyright and related rights violations (not specifically committed online) on a commercial scale (that is – piracy) are also provided. The directive provides remedies available to the rights holders in the EU Common Market. Although it generally codifies various remedies, available throughout the EU, it also introduces certain remedies, which were not previously used in some EU countries, e.g., public announcement of the fact of the infringement and the identity of the infringer at the expense of the infringer. Unfortunately, such entirely novel remedies in the Directive 2004/48/EC are not many. The majority of the regulated remedies are just uniformised existing remedies, known in the private tort law. Not entirely novel but important for enforcement of intellectual property rights are preventive action, said public announcements, court orders on disclosure of full information, securing of evidence before the lawsuit and in absentia of the infringer. No conceptually new sanctions for the infringement of intellectual property rights were introduced. All of these regulations and sanctions are generally derived from or related to the traditional judicial enforcement of intellectual property rights. Overall, the Directive 2004/48/EC provides offline protection for intellectual property rights, based on judicial or para-judicial legal proceedings and judicially administered sanctions. As a result, it has little direct means to impact the infringement on the internet, and especially to impact the dynamic and constantly evolving nature of the illicit activities with the digital content. The rules of the Directive 2004/48/EC also have no reach beyond the EU. In such dynamic and global environment traditional remedies are generally too ineffective, too slow, too complex and too expensive.

As it was noted already, after the EU Enforcement Directive 2004/48/EC, new remedies against infringement of intellectual property online have been introduced only at the national level and only in individual countries. After Directive 2004/48/EC only some legal novellas have emerged in the national law (such as the „three strikes“ approach) and further analysis will focus expressly on these novellas. Two principal remedy novellas shall be identified and analysed. The first one is the “three strikes” (also known as graduated response) remedy, originating in France.

The European Data Protection Supervisor has precisely summarized the approach as follows: "*copyright holders using automated technical means, possibly provided by third parties, would identify alleged copyright infringement by engaging in monitoring of Internet users' activities, for example, via the surveillance of forums, blogs or by posing as file sharers in peer-to-peer networks to identify file sharers who allegedly exchange copyright material. After identifying Internet users alleged to be engaged in copyright violation by collecting their Internet Protocol addresses (IP addresses), copyright holders would send the IP addresses of those users to the relevant Internet service provider(s) who would warn the subscriber to whom the IP address belongs about his potential engagement in copyright infringement. Being warned by the internet service provider (ISP) a certain number of times would automatically result in the ISP's termination or suspension of the subscriber's Internet connection.*"⁴

The second remedy for dealing with the IPR infringements is general filtration of the online information. Non-individual enforcement would require making the infringing internet content unavailable for large groups of users. Such enforcement in bulk seems to be possible through blocking or filtering of certain internet resources, which contain unauthorized content or facilitate access to such content (e.g., P2P sites). Blocking or filtering of the illicit content may be based on IP address and domain name (DNS) filtering, i.e., filtering all internet resources available under a specific IP address or domain name. A more recent approach is the DPI filtering, which involves live screening of the packets of data, which are being transmitted and received by the network hosts.

Research on internet blocking and filtering⁵ suggests that it has the potential to infringe fundamental rights, including privacy rights, which led the affected parties to the Court of Justice of the European Union (ECJ). The ECJ recently ruled on two cases pertaining to internet filtering for dealing with copyright infringements. The ECJ decision in the *Scarlet Extended* case C-70/10 formulated five criteria for when filtering is not deemed legally proportional, among them all embracing and non-discriminative filtering. The same principles were also extended to hosting service providers in the most recent ECJ *Netlog* case C-360/10 decision. These decisions in addition for enlightening the legal conditions for the internet filtering as a legal remedy, also expressly reiterate that IP addresses are personal data, which shall be subject to data protection laws, and cannot be controlled (collected), without complying with the data controller obligations.

The "three strikes" is essentially a lesser version of information control on the internet, since it requires certain monitoring of users' activities on the internet and is hence inherently incompatible with privacy. Moreover, the remedy envisaged by the "three strikes" approach is loss of the internet access, which is increasingly recognized as the novel "digital" fundamental human right⁶.

The final substantive legal act which shall be reviewed is the Anti-Counterfeiting Trade Agreement (ACTA). ACTA attempted to formalize new obligations (remedies) against online service providers, in order to involve them in identifying of the infringing subscribers. According to par. 4 Article 27 of the ACTA, online service providers may be ordered to disclose information on a subscriber whose account was used for infringement, thus enabling legal action against such subscribers. Con-

⁴ *Opinion of the European Data Protection Supervisor, On the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) (2010/C 147/01):* 3-4, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf last accessed on 15.03.2013 (2010).

⁵ *Internet blocking study, Internet blocking: balancing cybercrime responses in democratic societies study*, October 2009, http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf last accessed on 15 June 2012 (2009).

⁶ *Cerf, Vinton G., Emergent Properties, Human Rights, and the Internet*, *Internet Computing*, IEEE, 2012, 16.2: 87-88 (2012).

cerns that such provisions may not be in line with privacy rights⁷ have led to the European Parliament dismissing the ratification of ACTA in the EU. Principal problem with said ACTA rules is that they are not in line with the legitimate criteria for advanced collection of personal data (electronic identifiers or users, such as IP address), since the claims for infringement of intellectual property rights would only be raised post the collection⁸.

Both the “three strikes” and internet filtering/blocking at least partially resulted from the privacy caused frustrations and complexities of prosecuting individual infringers on the internet outlined above, however they do suffer from own privacy troubles as it is explained above. Moreover, the “three strikes” and filtering/blocking are not restorative remedies. They neither eliminate the source of the illicit content, nor ensure restitution of monetary harm. Assuming the current socio-economic environment and prevalence of the intellectual property infringements among the young and socially vulnerable (unemployed) people, there is no further remedies available (save for the imprisonment) for most internet users, if they continue to infringe intellectual property rights.

It must be noted that “three strikes” and filtering/blocking have adverse effect on the legal internet content, non-infringing internet users or even the society at large. Technical interference with the flow of information, monitoring and logging of IP addresses, and resources accessed by the internet users also raise general privacy concerns.

The analysis provided above suggests that current remedies available for enforcing intellectual property rights online are not privacy friendly and often are in direct conflict with users’ privacy rights and data protection requirements. This highlights the need for other remedies, which would address privacy concerns. The need is especially acute due to rejection of ACTA, which was significantly influenced by privacy concerns.

3. Reconciling privacy and intellectual property rights enforcement interests

In view of the privacy struggles of the analysed remedies, it is surprising that successful remedies in enforcing some intellectual property rights are not put to a wider use. Cybersquatting, a form of trademark rights infringement online, was efficiently remedied through specific new remedy involving mandatory assignment of domain names. These specific remedies are implemented and enforceable supranationally at the domain name system (DNS) level through the Internet Corporation for Assigned Names and Numbers (ICANN) and domain registrars. The Uniform Domain Name Dispute Resolution Policy (UDRP) is the specially created ADR process for the resolution of disputes regarding the registration of internet domain names and administering the above new remedy. The UDRP currently applies to all .aero, .asia, .biz, .cat, .com, .coop, .info, .jobs, .mobi, .museum, .name, .net, .org, .pro, .tel and .travel top-level domains, and some country code top-level domains, including .eu. Currently 65 country-code top-level domains (ccTLDs) have adopted the UDRP or a variation thereof and fall under the UDRP procedure administered by the WIPO Arbitration and Mediation Center⁹. With the most recent 2012 expansion of the top level domain names, the UDRP will extend as well.

According to the UDRP rules the ultimate ownership of the domain names (mandatory assignment thereof) is decided. For the purposes of the research in this article, it is most important that the UDRP procedure is generally compatible with the privacy of the parties, registering the domain

⁷ *Giannopoulou Alexandra*, Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality, *European Journal for Law and Technology*, Vol. 3, No. 1, 2012 <<http://ejlt.org/article/viewArticle/122/204> last accessed 15.03. 2013 (2012).

⁸ *Baraliuc, Irina; Depreeuw, Sari; Gutwirth, Serge*, Copyright enforcement in the digital age: a post-ACTA view on the balancing of fundamental rights. *International Journal of Law and Information Technology*, 21.1: 92-104 (2013).

⁹ *WIPO*, Domain Name Dispute Resolution Service for country code top level domains (ccTLDs), <http://www.wipo.int/amc/en/domains/cctld/index.html>, last accessed on 15.03.2013 (2013).

name – domain name registrants. Domain registration is a contractual process, where the domain name registrants enter into a contract with the registrar and concede the dispute resolution to the UDRP procedure. Thus, from the point of view of data protection the personal data is processed under the clear legitimate processing criteria established in Art. 7(b) of Directive 95/46/EC – when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract. This is legally very clear compared to vague legitimacy in situations when a third party is collecting private data about the internet user, who is suspected of intellectual property rights infringement.

As an example of the UDRP contractual rules, the rules for .eu set forth in the .eu Domain Name Registration Terms and Conditions (.euTC)¹⁰ shall be analyzed in detail. .euTC prescribe that the registrant has obligations to keep its contact information and e-mail functioning, accurate, complete and up-to-date; to use the domain name in such way that it does not violate any third party rights, applicable laws or regulations; not to use the domain name (i) in bad faith or (ii) for any unlawful purpose (Section 3). Also, the registrant represents and warrants that the request for Domain Name registration is made in good faith, for a lawful purpose and does not infringe the rights of any third party (Section 4).

.euTC in Section 11 contains specific rules regulating privacy and data protection. By registering a domain name and accepting the .euTC, the registrant authorises the domain registry to process personal data, which is required to operate the .eu domain name system. Besides the data use for normal domain name operations, personal data of the registrant may be transferred to third parties:

- 1) after the unambiguous consent of the Registrant
- 2) if ordered to do so by a public authority, carrying out its legitimate tasks,
- 3) upon demand of the ADR bodies authorized to resolve a dispute under Section 15 of the .euTC, or
- 4) if disclosure is needed for legitimate reasons, which are clearly stated and substantiated, and subject to special formalities.

Under Section 15 of the .euTC, the registrant accepts that the UDRP based ADR Procedures must be conducted before one of the entitled ADR providers. In case the ADR established a breach of third party rights, the remedies available through the ADR include revocation or mandatory transfer of the domain name.

It must be acknowledged that .euTC rules are much more specific with respect to the privacy and data protection matters, than the WIPO UDRP rules, however all UDRP derived ADR rules rely on the basic contractual grounds for the access to the registrants' personal data. In the domain contract the registrant must among other things accept that the applied for domain name "*will not infringe upon or otherwise violate the rights of any third party*", agree to accept the UDRP procedure, agree to the mandatory domain assignment in cases the contract is violated (third party intellectual property rights violation).

It must also be recognized that the registrant may opt to maintain privacy, at the expense of forfeiting (and thereby likely losing) the UDRP proceedings. Thus, if no actual personal data is made available for the registration of the domain name (e.g., the registrant uses privacy proxies) and the registrant does not respond to all UDRP communication, there is no legal way under the UDRP to identify such registrant, however the registrant is also non-compliant with the domain registration terms and therefore risks the cancellation or mandatory assignment of the domain, even without the infringement of the third parties' intellectual property rights.

¹⁰ Eurid, .eu Domain Name Registration Terms and Conditions (v.5), http://www.eurid.eu/files/trm_con_LT.pdf, last accessed on 15.03.2013 (2013).

Based on the above analysis .euTC and UDRP, as well as novel remedy available thereunder – seizure of online resource – domain name – are effectively compatible with the general data protection requirements and are adjusted to deal with the indirectly identifiable party problems and is generally aimed directly at the party involved with the infringement. A domain name, which may be used for illicit activities, is very close to the source of the infringement and may even be directly owned by the infringer. Domain seizure *per se* does not infringe on the privacy rights of the domain registrant, while conflicts with other rights of the user are also relatively limited. It is important to note that domain seizure does not affect the privacy of other internet users and the public at large, it does not interfere into the content of the online communication and does not increase the costs of online services and very rarely threatens legitimate internet content (e.g., several websites under one IP). For *prima facie* infringement cases it may offer efficient resolution with the well and in advance defined input on the side of the right's holder.

From the point of view of effectiveness and compared to other remedies, domain seizure is limited remedy. It does not restore the pecuniary harm, it still bears some costs which are non-recoverable, it suffers from jurisdictional limitations (it is possible for the perpetrator to switch to the domain outside the UDRP with minimal disruption) and it is currently focused on trademark law disputes. Certain rights closely related to trademarks, such as firm names, may also be enforced. Copyright and related rights, which form the bulk of intellectual property rights infringed online (but not in the domain names *per se*) are not directly enforceable through UDRP.

Since UDRP process and institutions are compatible with user privacy and least intrusive into the public privacy, it shall be considered for a greater use for intellectual property rights holders. Remedies available under this system - domain seizure and take-over – shall be considered to be made available for a broader use in intellectual property rights enforcement online, including copyright and related rights enforcement. As it was already noted, illegal content infringing copyright and related rights are generally provided and/or accessible under the domain name or internet resources available under (or associated with) the domain name. This assumption is valid even for P2P networks, which operate special P2P tracker servers. This focusing of legal coercion and remedies on domain names is appropriate, as long as the instrumental nature of the domain names is established.

Noteworthy additional benefit of domain seizure remedies under the UDRP process is that UDRP institutions have accumulated substantial expertise and precedent in establishing illicit use of domain names, which take into account the content (lawfulness or unlawfulness thereof) of the internet resources available under (or associated with) the domain name. The UDRP procedures rely on intellectual property law experts, enforcement expenses are rather insignificant and the remedies may be applied very hastily. The latter have already been recognized as key features for successful enforcement of intellectual property rights online¹¹.

Domain seizure remedy for infringements of copyright and related rights is not a panacea. Some significant limitations shall be noted, such as

- no possibility to deal with infringement in many national jurisdictions;
- difficulty in dealing with domain forwarding situations, i.e., where domain in friendly jurisdiction is forwarded to unfriendly jurisdiction;
- possibilities to abstain from domain use in intellectual property rights infringement online (e.g., through IP address based access).

The above limitations are generally applicable for any existing remedies, hence shall not be considered as disadvantages of the domain seizure remedy. Domain seizure therefore shall be an addition,

¹¹ Lemley, Mark A.; Reese Anthony R., Reducing Digital Copyright Infringement Without Restricting Innovation, 56 *Stan.L. Rev.* 1345, 1350–1434 (2004)

but not a replacement to the arsenal of other available legal remedies. It may be especially useful against the relatively limited number of sites that are either infringing or facilitating infringements of intellectual property rights and would allow certain marginalization of P2P and other infringing sites, since for the average user the domain names are primary conduits to access any content online.

Domain seizure remedy possessed significant advantages not only for privacy rights. It is also friendly general flow of information online (it will not interfere into the flow), it would be much more selective compared to blocking and filtering technologies, the economic costs to implement it would be marginal.

Adopting this remedy for the broader use in enforcement of intellectual property rights online would not require major substantive legal framework. In most European countries the private law legal remedies available to the courts are not exhaustive and limited in the law. Nevertheless, it may be very difficult to adopt this remedy at the court level, since significant overhaul of the civil procedure rules pertaining to anonymity and privacy of the defendants may be necessary. Online ADR procedure is already adapted to certain anonymity and privacy of the online users, hence it may be preferred to administer the domain seizure from the point of view of compatibility with the existing privacy and data protection laws and general privacy friendliness. Further step may be international expansion of these remedies in order to limit jurisdiction jumping and domain forwarding limitations and ensuring cooperation of the larger number of the national domain registrars. The latter is realistically achievable since domain registrars have no economic interest to protect and their number is much lesser compared to billions of internet subscribers and hundreds of thousands of online service providers. Most importantly, it shall not interfere or undermine user privacy, which is key parameter for exercising fundamental human rights online.

Seemingly, the potential of this novel remedy, as well as advantages to user privacy and other important interests are gaining broader recognition at the moment, when this article is being finished. Recent Hadopi proposals on enforcement of intellectual property rights online in France have embraced the domain seizure as a possible new remedy¹². Unfortunately, Hadopi is not concerned with making this remedy privacy compatible, but it rather focuses on its potential to be administered in an administrative or judicial way. These considerations shall be viewed as risky, since as it was noted in this paper the compatibility with user privacy is legally essential and shall not be an afterthought. Not accounting for user (domain registrant) privacy may cause abuse of this remedy, limit the useful applications thereof and even make it legally unacceptable, as it may run into the *Promusicae* and other fundamental rights defences. Existing online ADR vehicles, which already provide working mechanisms accounting for the domain registrant privacy, shall therefore be the primary means to administer the expanded applications of this remedy.

4. Conclusions

The remedies for intellectual property rights infringement are generally incompatible with user anonymity and privacy online. Online privacy rights are subject to extensive regulation in the EU, which causes legal difficulties in collecting, storing and other processing of user data, as well as unraveling the individual behind the digital identifiers (such as IP address), what is necessary for the judicial enforcement of intellectual property rights. These incompatibilities with user privacy are not addressed on the newest anti-piracy remedies – “three strikes” and internet filtering/blocking. On the contrary, they run into direct tension with user privacy and other fundamental rights as demonstrated in the ECJ's *Promusicae* and *Scarlet Extended*.

¹² HADOPI, Rapport sur les moyens de lutte contre le streaming et le téléchargement direct illicites, http://www.hadopi.fr/sites/default/files/page/pdf/Rapport_streaming_2013.pdf last accessed 15.03.2013 (2013)

The paper considers enforcement of trademark rights online through online ADR process based on UDRP rules and special remedy of domain seizure as a successful example of aligning privacy and enforcement interests. Domain seizure/takeover through the existing UDRP system is successful and generally privacy friendly remedy dealing with trademark rights infringement in domain names. It takes into account all the requirements of the EU privacy and data protection rules, it provides clear legal grounds to process registrant personal data and limits the scope of such processing, it allows the user to maintain privacy at the cost of losing his interests in domain name, it also has other advantages making it inherently more compatible with online privacy. Adoption of this remedy at the national court level may be very problematic, since significant overhaul of the civil procedure rules may be necessary.

Thus, expansion of the domain seizure through existing UDRP based process to broader use of intellectual property enforcement therefore may be useful privacy-friendly addition to the existing remedies, and would allow certain marginalization of infringement online, since for the average user the domain names are primary conduits to access any content online. Existing UDRP based process, already provides a working mechanism compatible with the domain registrant privacy. Therefore, it shall be considered as a preferred way to expand the use of domain seizure remedies in enforcing all intellectual property rights online.

5. References

Baraliuc, Irina; Depreeuw, Sari; Gutwirth, Serge, Copyright enforcement in the digital age: a post-ACTA view on the balancing of fundamental rights. *International Journal of Law and Information Technology*, 21.1: 92-104 (2013).

Bridy Annemarie, Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement. *Oregon Law Review*, Vol. 89, p. 81, 2010, http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID1698542_code630766.pdf?abstractid=1565038&mirid=1 last accessed on 15.03.2013 (2010).

Cerf, Vinton G., Emergent Properties, Human Rights, and the Internet, *Internet Computing*, IEEE, 16.2: 87-88 (2012)

Coudert Fanny; Werkers Evi, In the Aftermath of the Promusicae Case: How to Strike the Balance? *Int J Law Info Tech* 18 (1): 50-71 (2010).

Eurid, .eu Domain Name Registration Terms and Conditions (v.5), http://www.eurid.eu/files/trm_con_EN.pdf, last accessed on 15.03.2013 (2013).

Giannopoulou Alexandra, Copyright enforcement measures: the role of the ISPs and the respect of the principle of proportionality, *European Journal for Law and Technology*, Vol. 3, No. 1, 2012 <<http://ejlt.org/article/viewArticle/122/204> last accessed 15.03. 2013 (2012).

HADOPI, Rapport sur les moyens de lutte contre le streaming et le téléchargement direct illicites, http://www.hadopi.fr/sites/default/files/page/pdf/Rapport_streaming_2013.pdf last accessed 15.03.2013 (2013).

Internet blocking study, Internet blocking: balancing cybercrime responses in democratic societies study, October 2009, http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf last accessed on 15 June 2012 (2009)

Lemley Mark A.; Reese Anthony R., Reducing Digital Copyright Infringement Without Restricting Innovation, 56 *Stan.L. Rev.* 1345, 1350–1434 (2004).

Opinion of the European Data Protection Supervisor, On the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA) (2010/C 147/01): 3-4,

http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf last accessed on 15.03.2013 (2010).

Richardson Megan, Downloading Music off the Internet: Copyright and Privacy in Conflict? *Journal of Law and Information Science*, Vol. 13, No. 1, p. 90-106 (2002).

WIPO, Domain Name Dispute Resolution Service for country code top level domains (ccTLDs), <http://www.wipo.int/amc/en/domains/cctld/index.html>, last accessed on 15.03.2013 (2013).

SOFTWARE USABILITY AND LEGAL INFORMATICS

Anna Ronkainen

Chief Scientist, Onomatics, Inc.
Vuorikatu 14, 00100 Helsinki, FI
anna.ronkainen@onomatics.com; <https://www.onomatics.com/>

Keywords: *Human-computer interaction, usability, trademark databases, legal informatics, artificial intelligence and law, medical data systems*

Abstract: *This paper examines software usability from two different perspectives within legal informatics. Firstly, the current state of legal regulation of usability of medical systems is explored briefly. Secondly, different levels of usability in legal information systems are examined through two examples of trademark databases based on a high-usability represented model (TrademarkNow NameCheck from Onomatics) and the more traditional implementation model (USPTO TESS) with poor usability.*

1. Introduction

Software usability has received more and more attention over the last two decades as the role of computers in all aspects of our daily lives has become increasingly prominent. Our understanding of good usability has grown together with computer users' demand for it, and the state of the art in computer software design and hardware performance is no longer a limiting factor, either.¹

In this paper I review software usability in the legal context from two different perspectives. One is the issue of usability as an object for legal regulation. In this area there is very little earlier work available at the level of generality attempted here, as there is only patchwork legislation covering specific sectors of operation or the specific question of accessibility, that is, usability as it relates to particular groups of users with special requirements regarding modalities of access (e.g. visually handicapped people).

The second issue is the question of usability as far as legal information systems are concerned. What is the prevailing level of usability in legal information retrieval, and what is the state of the art? Is there a difference between the standard level of usability in the legal field and information retrieval in general?

2. What is usability?

The ISO 9241-210 standard² defines usability as follows: Usability is the extent to which a system can be used by specific users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use. An earlier definition was provided by Jakob Nielsen in his influential book Usability Engineering:

It is important to realize that usability is not a single, one-dimensional property of the user interface. Usability has multiple components and is traditionally associated with these five usability attributes:

¹ On usability in general, see e.g. Norman 1998, Norman 2011, Vicente 2004, Vicente 2011, Goodwin 2009, Cooper *et al.* 2007.

² ISO 9421-210: Human-centred design processes for interactive systems, 1999, formerly ISO 13407.

- Learnability: The system should be easy to learn so that the user can rapidly start getting some work done with the system.³
- Efficiency: The system should be efficient to use, so that once the user has learned the system, a high level of productivity is possible.
- Memorability: The system should be easy to remember, so that the casual user is able to return to the system after some period of not having used it, without having to learn everything all over again.
- Errors: The system should have a low error rate, so that users make few errors during the use of the system, and so that if they do make errors they can easily recover from them. Further, catastrophic errors must not occur.
- Satisfaction: The system should be pleasant to use, so that users are subjectively satisfied when using it; they like it.⁴

Nielsen advocated focusing on objectively quantifiable aspects of usability at the expense of user satisfaction, which in the last few years has received increased attention as a central part of user experience (UX) design. And, as mentioned earlier, accessibility can also be seen as a special case of usability. The umbrella term for all this is human-computer interaction (HCI).

The case for usability should be obvious. In Finland, according to the National Audit Office⁵, up to 400.000 doctor's appointments' worth of working hours are lost because of poor usability in the medical sector alone. Poor usability is naturally also undesirable from the perspective of occupational well-being. In the medical sector in Finland, again, this issue has already been subject to extensive surveys. In one⁶, the average grades given to different patient record systems in terms of usability ranged from 6.1 to 7.2 (and one outlier at 8.4) on a scale of 4 (worst) to 10 (best), with all the most widespread systems at the bottom end of the scale. The findings were summarized as follows:

Systems lacked the appropriate features to support typical clinical tasks, such as decision making, prevention of medical errors, and review of a patient's treatment chart. The systems also required physicians to perform fixed sequences of steps and tasks, and poorly supported the documentation and retrieval of patient data. The findings on ICT support for collaboration showed mainly negative results, aside from collaboration between co-located physicians. In addition, the study results pointed out physicians suffering from system failures and a lack of integration between the systems.⁷

While some of these complaints are specific to the clinical setting, some of them must sound familiar to lawyers as well. Usability of legal information technology has never received similar attention from researchers, if, indeed, any at all. Providers of large-scale legal IT systems must certainly carry out at least some research of this type in the interest of product development, but for commercial reasons it rarely reaches publication.

3. Legal regulation of usability

Usability is already subject to legal regulation in certain contexts. In this paper I briefly outline the regulatory situation as far as Finland or the EU is concerned for one specific area, namely medical data systems. This is by far not intended as a comprehensive treatment of the topic in general.

³ At the time of writing this one-way conception was the only feasible interpretation of learnability. Nowadays learnability can also be expected of intelligent systems in that they can learn certain behaviours of the user and make them more efficient.

⁴ Nielsen 1993, p. 26.

⁵ http://www.vtv.fi/ajankohtaista/tiedotteet?3680_m=3546 (last accessed 2013-03-15).

⁶ Viitanen *et al.* 2011.

⁷ Viitanen *et al.* 2011, pp. 708-709.

Standards with specific requirements concerning human-computer interaction are legally binding in some other safety-critical contexts as well, such as the controls of a railway locomotive.⁸

In the EU, the safety of medical devices is regulated by the Medical Devices Directive.⁹ In Finland, this is implemented by the Medical Supplies and Equipment Act (629/2010). The directive¹⁰ and, indirectly, the Act require that medical equipment conform to the applicable standards regarding product safety. The latest revision of the list counts approximately 350 different standards.¹¹

Medical software is now unambiguously within the field of application for the directive and the act.¹² One of the standards with which compliance is required concerns usability specifically.¹³ This standard was developed under the auspices of the Association for the Advancement of Medical Instrumentation. This standard mandates the use of several generally accepted usability-oriented design practices.

That the usability of medical software is a safety concern is unquestionable. One third of the Finnish doctors surveyed reported that poor usability caused or nearly caused a serious injury to a patient.¹⁴ One recent case which received wide publicity in Finland concerned the interaction of one (or, in theory, any) patient record system and the national electronic prescription system currently being introduced: a line break in the dosage instructions written by the doctor would be misinterpreted at the pharmacy end so that the preceding character would be written twice, so that for example “2 tablets” could become “22 tablets”.¹⁵ As a consequence, the National Institute of Health and Welfare issued a temporary ban on the use of the line break in prescriptions (sic!), and the use of electronic prescriptions altogether was put on hold at least in one municipality.

The acceptance procedure for non-invasive devices, including most medical software products, is based on self-supervision: the manufacturer has to submit an EC Declaration of Conformity, including required technical documentation, before the product is released.¹⁶ If non-compliance is detected afterwards, the use of the device may be prohibited or the manufacturer may be required to correct the deficiencies.¹⁷ In extreme cases, criminal liability (fine) is also possible.¹⁸ According to the National Audit Office, the supervisory system is non-existent as far as medical data systems are concerned, and there are no plans to require conformance for pre-existing systems.¹⁹ Only major new releases trigger the requirement. The extension of the Medical Devices Directive should have taken full effect in March 2010.²⁰

The Commission has submitted a proposal for a new Medical Devices Regulation²¹ on 26 September 2012.

⁸ CLC/TS 50459:2005, authorized by 28 § 2 of the Railways Act (555/2006) through the administrative decree RVI/873/410/2009. On the other hand, the standard EN 60964:2010 on the design of nuclear power stations' control rooms does not (yet) seem to be legally binding.

⁹ Council Directive 93/42/EEC of 1993-06-14 concerning medical devices.

¹⁰ Article 5.

¹¹ EU OJ C 242, 2011-08-19, pp. 8–38.

¹² Article 1 paragraph 2 point a of the Directive as amended by Article 2 of 2007/47/EC, and 5 § 1 item 1 of the Act.

¹³ EN 62366:2008 Medical devices - Application of usability engineering to medical devices, originally ANSI/AAMI/IEC 62366:2007.

¹⁴ Viitanen *et al.* 2011, p. 718.

¹⁵ Ahlblad 2012.

¹⁶ Annex VII of the Directive.

¹⁷ Chapter 8 of the Act.

¹⁸ Section 59 of the Act.

¹⁹ Performance audit report 217/2011: The implementation of national IT projects in social and health care, pp. 48–54

²⁰ The amendment Directive 2007/47/EC, Article 4.

²¹ Proposal for a Regulation of the European Parliament and of the Council on medical devices, and amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009, 2012/0266 (COD)

Usability can also be a decisive factor in a case even absent positive regulation. This was the situation in the case about the Finnish e-voting trial²², in which the system – which had not been subject to any proper usability review – gave to hundreds of users the impression that a ballot had been cast even though it was waiting for final confirmation. Because of this, the Supreme Administrative Court ordered that the entire election be repeated in the three municipalities where the system was in use.

4. Usability of legal information systems

For lawyers, software usability has not become a hot topic of discussion in the same way as in the medical community. Is this because there is nothing worth complaining about? Hardly. My personal indicator for usability in Finnish legal information systems is whether any (or, hopefully at some point, all) of the major databases provide support for the inflectional morphology of the Finnish language. At the time of writing, none of the major three (Finlex, Edilex, Suomen Laki) services do. In these days²³ incorporating this feature is not rocket science, and high-quality implementations are even available as open source software.²⁴ Instead, users seem to be happy with just truncation. To see why this does not work, just consider the word *tie* (road). Using the stem in a wildcard search *tie** also captures words such as *tiede* (science) and *tietokone* (computer) while at the same time failing to find non-nominative plural forms of *tie*, such as the genitive *teiden*.²⁵ As a consequence, even the relevance-ranked search of Suomen Laki returns two statutes related to data protection (*tietosuoja*) at places 5 and 7 when searching for *tie*.

So what else could be the explanation? Is it just a lack of technical sophistication and consequently a lack of understanding of what is feasible, especially in the older generation of lawyers? An expression of the general conservatism exhibited by the profession? Or the point of view that even the current services are so much better than the traditional IR technologies involving collections of printed matter and copious use of the copying machine? Perhaps. The last one could certainly explain much of the difference with the medical profession, where the benefits of information technology may in some contexts seem questionable altogether. But indeed the legal profession seems to exhibit a peculiar form of blindness towards the sensibility of inherited practices, whether regarding established business models²⁶ on a more general level, or even the most arcane details of legal practice²⁷, a fact which somehow never ceases to amaze the non-lawyers amongst my colleagues and external partners at Onomatics.

One last possibility is that lawyers are indeed aware of the usability problems and in good lawyerly fashion invent creative ways to circumvent the problems. For information retrieval, the most obvious solution is to rely on the results provided by advanced general-purpose search engines such as Google or Bing. When documents from authoritative sources do not receive a prominent place among the search results, there may be tendency to rely on whatever the search does return instead. Hans Christian Spies has presented some evidence of this already happening in practice.²⁸ In the end this effectively means that the hallowed doctrine(s) of legal sources are replaced by Google's search algorithms. This can be particularly problematic when certain central types of legal sources

²² KHO:2009:39, see Hietanen *et al.* 2012

²³ As opposed to 20 years ago. But for comparison, the electronic archives of the largest Finnish daily newspaper Helsingin Sanomat have offered this feature since the late 1980s.

²⁴ Such as the HFST toolkit, <http://www.ling.helsinki.fi/kieliteknologia/tutkimus/hfst/> (last accessed 2013-03-15)

²⁵ All the other non-nominative plural forms of *tie*, such as the partitive *teitä*, are homographic with the second-person plural pronoun *te*. Syntactic disambiguation is obviously the required next step to get rid of this stop word.

²⁶ Susskind 2008.

²⁷ Such as the widespread firm belief in the superiority of fax machines over more modern forms of electronic communications.

²⁸ Spies 2010.

are only made available by commercial publishers and put behind a paywall, thus not being indexed by search engines nor appearing in the search results. This is the situation with case law in Denmark, and Spies notes (and welcomes) a tendency to rely more on the freely available travaux préparatoires than precedent, in which a given decision may after all have been reached based on circumstances not present in most other cases of a similar kind. In Finland the situation is not as bad, but still one can ask whether it is desirable that the most convenient way to any source of Finnish law (except for legal doctrine) goes through Google. Of course this question can also be answered in the affirmative, in which case the possibility of active cooperation with search providers as a primary channel of information delivery should not be ruled out. For example, the USPTO already uses Google as a distribution channel for its bulk data products, whereas the EPO is cooperating with Google in a more ambitious project using a customized version of Google Translate as a tool for delivering translations of patent documents.²⁹

The effect of usability considerations in systems design can be illustrated by comparing two interfaces to trademark search systems in Figures 1 and 2.

Figure 1: The USPTO Trademark Electronic Search System (TESS)

²⁹ Huttunen & Ronkainen 2012, p. 337n21.

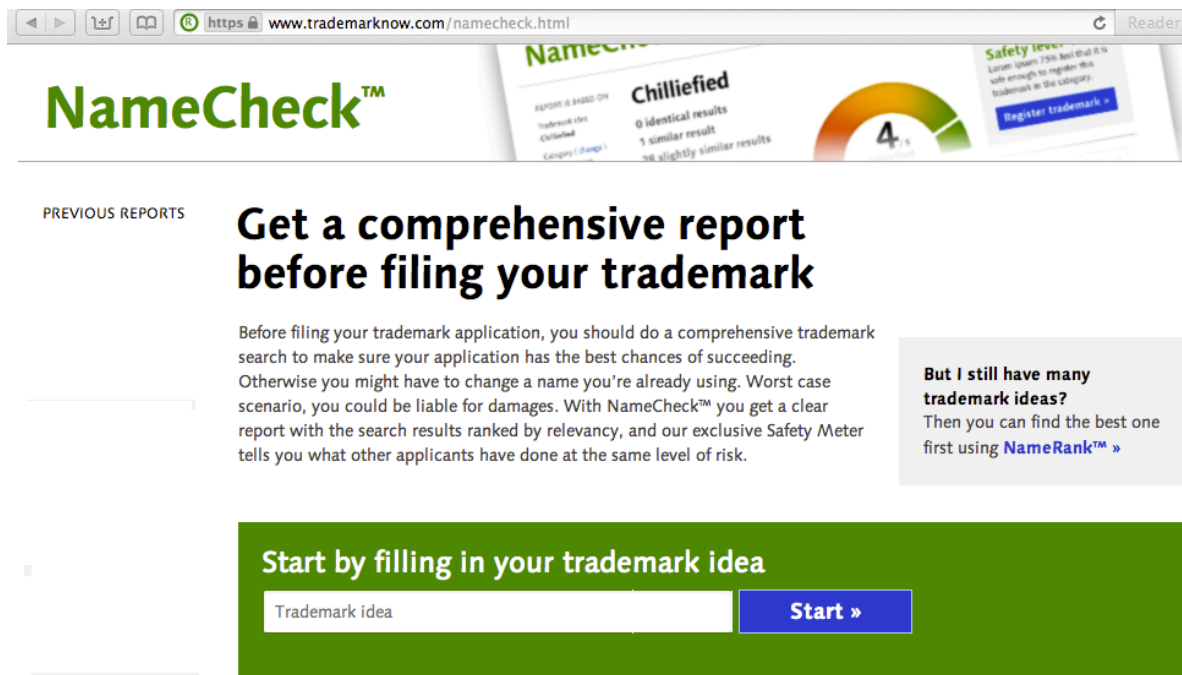


Figure 2: TrademarkNow NameCheck by Onomatics

Certainly the visual design (or lack thereof) is the most salient difference, but that is not the point. The wealth of fields and options might make one think the first system is much more powerful, but for all but a handful specialist users (who can perform even more configurable queries outside of this “New User (Basic)” search page), the converse is actually the case. In the second system, the complexity is not presented to users as choices they are forced to make beforehand without fully understanding them, but rather the query is interpreted appropriately, and the system’s artificial intelligence makes sure the results are presented in the most relevant order for making a likelihood of confusion (relative grounds) assessment.

These two examples are good illustrations for general design practices leading to different levels of usability. The USPTO system (Figure 1) is clearly based on an *implementation model*³⁰ or a *system model*, that is, the user interface (UI) closely mirrors the technical characteristics necessary for implementing certain functionalities. If the system is a trademark database, you design the user interface to do queries from the database. The “New User (Basic)” interface allows only a limited subset of queries, whereas the “Structured” interface permits any exact or wildcard query from any specified field(s) and any Boolean combination thereof. The next logical step on this trajectory would be to skip the web UI altogether and only allow users to perform queries using for example SQL. This in turn would not be all that far off from the UIs all legal information systems had circa 1990. At that time, such UIs were still state-of-the-art, limited by both the performance of the available hardware and the progress of computer science.³¹ This is no longer the case.

The TrademarkNow NameCheck (Figure 2), on the other hand, uses a high-level *represented model*³², which seeks to approximate the user’s *mental model* or *conceptual model*³³ for the task at hand. The underlying low-level implementation may be the same as in the implementation model, but added layers of intelligent technology enable the system to deal with questions typical users actually want answered. In the case of a trademark database, users either want to find some specific mark

³⁰ Cooper *et al.* 2007, p. 27 et seq.

³¹ One peculiar relic in the TESS UI is the logout button, which may have made good sense in the 1980s, but certainly not anymore, especially as the system requires no specific interaction to log in.

³² Cooper *et al.* 2007, p. 29

³³ Norman 2011, 34 et seq.

they know exists, which is easy enough with the basic database model as well, or to see what are the nearest marks for some mark, either to see that the risk for applying to register it is acceptable or to make sure there are no applications too close to one's existing mark. This in turn requires some computational representation of the specific legal issue at hand, namely trademark similarity or likelihood of confusion.³⁴ Finding the nearest marks in the legally relevant sense requires two inputs, the mark itself and the goods and services for which the mark is registered, and this is all the system asks from the user at the first stage, one at a time. It is worth noting that the implementation model may concern not only details of the technical implementation but also those of the legal implementation of the domain in question as well. In this case, one such detail is the international Nice classification of goods and services. Rather than require the users to be familiar with it, on the query side products can be input in natural languages, with text completion enabled and based on "normal" names for the products rather than verbatim entries from the official classifications, and on the results side they are also represented with icons. The class numbers are supported and displayed as well, but already the unevenness of the classification itself makes it rather impractical.

This type of mental-model-oriented abstraction has the downside of not permitting complex one-shot queries such as "find all marks filed between dates a and b which have been opposed based on provision c". For the benefit of users interested in and capable of performing such queries – legal scholars – it is of course desirable that implementation model interfaces remain available as well. Still, they should become the exception rather than the norm.

5. Conclusion

One problem with good usability is that it is unobtrusive and thus unnoticeable. The Google search box does not look any different from a database query or full-text search box. Also, when the design choices resulting in good usability are reviewed after the fact, they typically seem quite obvious, and this makes it easy to grossly underestimate the effort required to produce them. On the project level, this in turn may make it easy to forget to include the earliest stages in the design process, which are critical for the successful completion of the project. In this regard, more education is needed. The use of 21st century project management techniques³⁵, as opposed to the waterfall model³⁶, at the same time both enables and necessitates good design practices.

The legal system could certainly use a bit more design thinking³⁷ in general. The design perspective is unavoidable when having to start with what essentially amounts to a blank slate.³⁸ In stable legal systems, such opportunities rarely emerge spontaneously. Even the last great codification processes mainly sought to rewrite existing law without too many substantive changes. Design thinking could certainly also be used for less revolutionary changes.³⁹ One candidate for this was mentioned earlier in this article: the Nice classification of goods and services may have served a useful purpose when the system was introduced and trademark registers pushed the limits of index card technology. Also the product categories clearly show their age, and only making small incremental changes in them, such as the recent addition of classes 43 to 45, does not really solve anything. Nowadays there are better ways to deal with the task of grouping and retrieving similar products through intelligent technology.

³⁴ In this respect, TrademarkNow NameCheck is a further development of the work described in Ronkainen 2010.

³⁵ See e.g. Shore 2007.

³⁶ Even originally only intended a caricature of bad project management practices, Royce 1970.

³⁷ See e.g. Lockwood 2010.

³⁸ For example, a seminar titled Constitutional Design, inspired by the drafting process of the new Egyptian constitution, was arranged in Helsinki in May 2012.

³⁹ One example of such an undertaking is the Australian Integrated Tax Design Project, see Preston 2004.

If using Google is the easiest way to find legal sources, trying to stop people, even legal decision-makers, from using it is an unrealistic proposition. If access to legal sources is in practice left at the whim of a general-purpose search engine, the results may be catastrophic as far as legal certainty is concerned. On the other hand, intelligent legal technology has great potential for improving critical factors such as access to justice, and possibly even the quality of judicial decisions. None of this will become reality without proper usability, which will not be made a priority without demanding users. Certainly the legal profession has the right to expect high quality of their computerized tools, just as the medical profession.

6. References

- Ahlblad, Jaana. Vaara vaani rivinvaihdossa. *Suomen Lääkärilehti*, 67, 1472–1474 (2012).
- Cooper, Alan, et al. *About Face 3: The Essentials of Interaction Design*. Wiley, Indianapolis (2007).
- Goodwin, Kim. *Designing for the Digital Age: How to Create Human-Centered Products and Services*. Wiley, Indianapolis (2009).
- Hietanen, Herkko, et al. Vastuu sähköisen käyttöliittymän virheestä vuoden 2008 kunnallisvaalien äänestyksessä (Liability for user interface errors in the voting of the 2008 municipal elections). *Oikeus*, 41, 65–85 (2012).
- Huttunen, Anniina, & Ronkainen, Anna. Translation Technology and Copyright. *Nordiskt Immate-riellt Rättsskydd*, 330–344 (2012).
- Lockwood, Thomas (ed.). *Design Thinking: Integrating Innovation, Customer Experience, and Brand Value*. Allworth Press, New York (2010).
- Nielsen, Jakob. 1993. *Usability Engineering*. Academic Press, Boston (1993).
- Norman, Donald A. *The Design of Everyday Things*. MIT Press, Cambridge, MA (1998).
- Norman, Donald A. *Living with Complexity*. MIT Press, Cambridge, MA (2011).
- Preston, Alan. Designing the Australian Tax System. Pp. 208–213 of: Boland, Jr., Richard J., & Collopy, Fred (eds.), *Managing as Designing*. Stanford University Press, Stanford (2004).
- Ronkainen, Anna. 2010. Mosong, a Fuzzy Logic Model of Trade Mark Similarity. Pp. 23–32 of: Wyner, Adam Z. (ed), *Proceedings of the Workshop on Modelling Legal Cases and Legal Rules*.
- Royce, Winston. Managing the Development of Large Software Systems. Pp. 1–9 of: *Proceedings, IEEE WESCON* (1970).
- Shore, James. *The Art of Agile Development*. O'Reilly, Sebastopol, CA (2007).
- Spies, Hans Christian. Armlængdens lov. Pp. 85–94 of: Henrichsen, Carsten, et al. (eds), *Ret, in-formatik og samfund: festskrift til Peter Blume*. Jurist- og Økonomforbundets Forlag, København (2010).
- Susskind, Richard. *The End of Lawyers? Rethinking the Nature of Legal Services*. Oxford Univer-sity Press, Oxford (2008).
- Vicente, Kim. *Human Factor: Revolutionizing the Way We Live With Technology*. Vintage Cana-da, Toronto (2004).
- Vicente, Kim J. *Human-Tech: Ethical and Scientific Foundations*. Oxford University Press, New York (2011).
- Viitanen, Johanna, et al. National questionnaire study on clinical ICT systems proofs: Physicians suffer from poor usability. *International Journal of Medical Informatics*, 80, 708–725 (2011).

LINKING AND COPYRIGHT

Brita Kristina Herler

J Dr.Sc.(Econ, Law), University Lecturer, University of Vaasa, Finland
Street Number Wolffskavägen 34, 65200 Vasa, Finland (Pb 700, 65101 Vasa, Finland)
brita.herler@uva.fi; <http://www.uva.fi/en/profile/?view=1041516/>

Keywords: *Copyright, linking*

Abstract: *One of the problematic phenomena of the open network in recent decades from a copyright point of view has been the illegal distribution of musical and cinematographic works. Copyright infringements on networks and using computer systems have even become a larger problem than the sale of pirate copies of sound and picture recordings. Collecting, linking and integrating text, pictures, sound or multimedia, with or without frames, is an instance of making the material accessible to the public and of the user making a copy of it. On the contrary using hyperlinks is possible for internet users. The owner of a website may, without the authorisation of the copyright holders, redirect internet users, via hyperlinks, to protected works available on a freely accessible basis on another site.*

1. Inledning

En av det öppna nätverkets problematiska fenomen ur upphovsrättslig synvinkel har under de senaste årtiondena varit den allmänt kända tillkomsten av olaglig nätverksförmedling av musikaliska verk och filmverk. Noterbart är även hur de serverlösa nätverken har indelats i olika varianter, fråga har varit om ett medlande system, där en spindel i webben levererar sök och hämtande funktioner, eller det pekas ut användare för andra användare och erbjuds hjälp och varianter där deltagare i nätverket är på lika eller olika nivå, eller hur man åker snålskjuts, samt hybridssystem, där det inte existerar någon central förmedlare. Dessutom förekommer s.k. kardborrar som fäster allt avsett och utpekad angivet material.

Vid användning av differenta fildelningsprogram görs enligt de nordiska upphovsrättslagarna intrång om man utan upphovsmannens tillstånd decentraliserat kopierar eller laddar ner upphovsrättsligt skyddade verk. Likaså då man med tillhjälp av fildelningstjänster olovligen bjuder ut musikaliska och film- samt övriga skyddade verk ut för att kopieras av allmänheten eller en grupp personer, som inte på förhand är individuellt bestämd.

Det som dock den vanliga användaren av digitala nätverk mest berörs av är huruvida man kan utnyttja skyddade verk i samband med skapandet av arbetsrelaterat material och därmed tillgängliggörande för allmänheten. I de flesta fall rör sig frågan då om länkproblematiken i upphovsrätten. Det, hur man å andra sidan utnyttjar olika tekniker, exempelvis nätsyndikatorer, fildelning eller kardborrar, korrelerar inte med de ursprungliga länkarna.

Om länkar har det skrivits mycket och varierande. Terminologin har dessvärre inte varit genomgående enhetlig och en viss systematik har saknats i framställningen.¹ En klarläggning av länkar bör helst öppnas ur informations- och datorrättslig synvinkel med upphovsrättsliga förtecken, för att kunna besvara några av de frågor som idogt ställts under årens lopp.

¹Se t.ex. KB 2012:2, Pihlajanrinne 2011 och Levin 2011: 183–184 .

2. Länkteknik

Länkarna är måhända några av de mest säregna dragen i Internet. Med länkars hjälp kan man behärska en stor informationsmängd, eftersom länkarna håller ihop de olika, väsentliga dokumenten. Exempelvis för att produktinformationen skulle nå en större målgrupp och få en bättre effekt var länkarna en ypperligt god möjlighet till spridning av informationen. Dock utgör just avsaknaden av information ett av de problem användaren stöter på. Allt som oftast finner man s.k. döda länkar, från Gentscheins amerikanska urkälla till handelsplatsen vid Apple.com.² Dels blir källhänvisningen i forskningen haltande och dels kan konsumenten återopa sin rätt till information och tillgänglighet i näthandeln. Man kan överblicka hur, i takt med Internets kommersialisering och dess explosionsartade spridning, frågeställningarna kring den upphovsrättsliga relevansen av länkar över nätet tog fart.³

Fortfarande utgår man från HTML. Se t.ex. <URL: <http://www.w3.org>>. är kodspråket för att skapa ett hypertextdokument att användas i Internet. Länken kan vara en figur, som innehåller hypermedia, i vilken ingår bilder, ljud och text eller andra rörliga element (multimedia). Koder, såsom identifieringsnummer och symboler till information utgör även länkar.

Vid länkning är det tänkbart att vara obunden av sidindelning eller dylikt. Användaren ges vid HTTP möjligheter både till förflyttning från ett dokument till ett annat, dvs. hänvisningar från en webbsida i Internet till en annan sida (s.k. vanlig länk) och till en hämtning av material från en annan sida (s.k. hämtande länk). Man har använt benämningen länkar för dessa olika länkteknikbegrepp, fastän de är helt olika företeelser. Denna indelning bildar kärnpunkten i länkarnas upphovsrättsliga dilemma och med dessa insikter torde man ha kunnat analysera och bevaka de upphovsrättsliga intressena vid intrång under de senaste 15 åren.

I HTML-språket infogas kommandon i en textfil. I det fall, då webbläsaren helt lämnar länksidan och fyller bildskärmen med måldokumentet, på en tydligt angiven adress, talar man således om en vanlig länkning. Sådan länkning kan jämföras med uppgifter om ett telefonnummer eller hänvisningar i litteraturen. Skillnaden är dock att det är väsentligt mycket enklare att nå måldokumentet via länkar, än att på traditionell väg söka efter referenser. Denna typ av länk kan sägas hänvisa till annat material.

Hypertextdokumenten är textfiler, som innehåller endast text och olika koder eller HTML-märken. Man kan skriva dem med vanligt textbehandlingsprogram. Dessa textfiler innehåller inte ljud och bild. Ljud- och bildfilerna skall sparas såsom egna filer.

Vid den hämtande länktypen integreras bild- och ljudfiler i länkläggarens dokument. Med hjälp av ett särskilt kommando hämtar man bild, ljud o.a. material. Länkläggaren kan lägga på sin sida en s.k. inline-bild, -ljud etc. med vederbörande kommando, vilket hämtar en fil som innehåller t.ex. en bild eller ljud (ett musikaliskt verk eller ett filmverk). Dessa visas eller framförs automatiskt då användaren besöker länkläggarens sida.

Med hjälp av frameset-elementen (ram-element) kan man indela webbläsarfönstret i självständiga delar (ramar), för att kunna visa upp olika sidor. Till ramarna kan man hämta olika dokument (bild, text, ljud eller multimedia). Då varje ram fungerar som en självständig sida kan exempelvis dess innehåll bestämmas med kommandot. Det måldokument, som hämtas kan finnas på samma server eller nås med URL-adress. Till varje enskild ram kan man med ett kommando hämta olika material.

²Se Gentschein 1997: 20–21.

³Se Herler 2001: 203–223, 2011: 184–200 och Herler & Streng 2010: 87–117.

Det kallande dokumentets material ligger kvar då måldokumentet hämtas in i den bestämda ramen. Användarens egen webbläsare hämtar måldokumentet. Bildskärmens innehåll kan också flyta ihop, så att det är svårt att särskilja de olika dokumenten, eftersom kantlinjerna kan tas bort med kommandot för bildelementets border-attribut. Kantlinjerna är nämligen inte alls behövliga i materialhämtningen. Det enklaste sättet att föga en ljudfil till en sida, är dock att spara i filkatalogen och därefter hämta den med t.ex. <BGSOUND> märket. Ljudfilen innehåller ett musikaliskt verk, som är i digital form. Ljudfilen är i allmänhet relativt anspråkslös, men delvis genom utvidgade webbläsare och program har ständiga kvalitetsförbättringar beträffande ljudet skett.

3. Upphovsrättsliga överväganden

3.1. Vanliga länkar

Upphovsrättsligt relevant i sammanhanget är, att den användare som via en vanlig länk förflyttas till måldokumentet, inte framställer exemplar av måldokumentet hos länkläggaren. Efter förflyttningen är användaren i direkt förbindelse med måldokumentet och inte med länksidan. Man kan säga, att intrång i upphovsmannens ensamrätt att förfoga över verket beträffande exemplarframställning och tillgängliggörande för allmänheten, i allmänhet inte aktualiseras när det gäller den som skapat den vanliga länken. Däremot framställs exemplar hos utnyttjaren, men inte hos länkläggaren, t.ex. för utnyttjarens enskilda bruk. Detta beror på att en vanlig länk ger åt användarens webbläsare måldokumentets domain- eller URL-adress. På basen av denna adressuppgift hämtar användarens egen webbläsare (browser) direkt måldokumentet och visar det på användarens bildskärm. Ett möjligt verksexemplar framställs av användarens egen webbläsare och detta verksexemplar är fäst vid minnesområdena på användarens egen möjäng och möjligtvis i den server eller tjänst som han använder. Detta verksexemplar framställs inte av den vanliga länkläggaren. Han ger endast en adressuppgift, var man kan finna filen eller webbsidan som tillgängliggjorts för allmänheten. T.ex. i målet Stockholms Tingsrätt 11.6.2010 *Svensson m.fl. v. Retriever Sverige AB* behandlades en tjänst, som man med sök- och spårningsverksamhet kunde följa nyheter. Man erbjöd även en länklista med artiklar. Domstolen konstaterade, att eftersom det utgjorde en vanlig länk, aktualiserades inte ett tillgängliggörande för allmänheten. Svea hovrätt hade framställt en begäran om förhandsavgörande i ärendet. EU-DOMSTOLEN (fjärde avdelningen) avgjorde ärendet i mål C-466/12: **Artikel 3.1 i Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 ska tolkas så, att tillhandahållandet på en webbplats av klickbara länkar till verk, som är fritt tillgängliga på en annan webbplats, inte utgör överföring till allmänheten på sådant sätt som avses i denna bestämmelse.**

Målsidan öppnas i användarens digitala möjäng alldeles på samma sätt som om användaren själv skulle ha skrivit målsidans URL-adress i sin webbläsare. Användaren ser i möjängens bildskärm webbläsarens meddelande om, att webbläsaren söker nya webbsidor och att användaren har kommit till en ny sida då kontakt erhållits. En vanlig hypertext-länk får inte till stånd något extra i upphovsrättslig mening. I Finland har man ansett, att målsidans upphovsman har gett sitt samtycke till en normal Internet-användning av sidan, då han lagt ut sin webbsida på en server för allmänheten utan begränsningar. Denna uppfattning verkar vara motiverad. Till webbsidornas normala användning hör, att användarna fritt kan ta kontakt med sidan samt bläddra, titta och läsa sidor och dessutom printa ut på papper t.ex. för eget bruk. Till allmänt förfarande hör också, att målsidans upphovsman sätter klara begränsningar på sin

sida, om han inte tillåter att den används fritt. Detta kan ske genom användarsignum och lösenord, tekniska spärråtgärder eller att med begränsningar göra klara noteringar vid ifrågavarande webbsidor. Detta har även domstolarna i sina motiveringar hänvisat till, exempelvis i avgöranden Bundesgerichtshof 19.10.2011, I ZR 140/10 (*Vorschaubilder II*), Bundesgerichtshof den 17.7.2003, mål IZR 259/00 (*Paperboy*) och Bundesgerichtshof 29.4.2010, mål I ZR 69/08 (*Google*). I den sist nämnda fann domstolen uttryckligen att upphovsmannen gjort materialet fritt tillgängligt för sökmotorer och inte skyddat sig med tekniska åtgärder. Dock ansågs det betydelselöst i fallet Cour d'appel de Bruxelles, 5.5.2011, *Copiepresse v. Google*. Men däremot kringgående av tekniska skyddsåtgärder utgör intrång i rätten till tillgängliggörande, såsom i Bundesgerichtshof den 29.4.2010, mål I ZR 39/08, *Internetkartor*.

Användaren och den som gör en vanlig länk har således en motiverad orsak att anta, att en vanlig användning av webbsidan är tillåten, ifall inga begränsningar har gjorts eller märkts på sidan. Verket blir också offentliggjort, då det på upphovsmannens initiativ sparas på Internet-servern tillgängligt för allmänheten utan begränsningar.

Målsidans upphovsman har kunnat förena t.ex. en musikfil till målsidan, vilken automatiskt spelar bakgrundsmusik för att underhålla webbsidans besökare. Detta är ur upphovsrättslig synvinkel problemfritt, om målsidans upphovsman själv skapat musiken eller om han har fått tillstånd att framföra den. En vanlig länk för användaren till denna målsida på samma sätt som om användaren själv skulle ha letat efter målsidan. Man tar del av verket, t.ex. lyssnar på musiken eller ser bilder på målsidan på det sätt som målsidans upphovsman har avsett. En vanlig länk till en dylik sida är bara ett givande av adressuppgifter till användaren, så att användaren hittar till en sida, som upphovsmannen själv har tillgängliggjort för allmänheten. Framförandet av musiken sker inte på grund av länkläggarens åtgärder. Målsidans upphovsman har själv gjort det valet, att användarna hör hans musik, ser hans bilder eller läser hans texter. För att göra en vanlig länk behövs, förståeligt nog, inte under dessa omständigheter särskilt tillstånd.

En upphovsman till verk kan på sin webbsida lägga ut ett flertal verk, bland vilka Internetanvändaren kan genom att klicka välja ett verk enligt tycke och smak. Upphovsmännen kan ha som avsikt, att de tack vare denna gratisutdelning blir berömda och når publicitet. Att lyssna på musik i användarens egen sfär gör inte intrång på upphovsmannens upphovsrätt. Upphovsmannens samtycke förutsätts för att framföra detta verk offentligt. Att göra en länk till en dylik webbsida kan inte anses vara framförande av verk. Verkets upphovsman har själv tillgängliggjort sitt verk för allmänheten. Användaren sätter igång framförandet av exempelvis musiken med upphovsmannens samtycke. Samma synpunkter omfattar också den situationen, att upphovsmannen till ett verk har lagt sina verk på en server för att kopieras av Internetanvändare. Det är tillåtet att kopiera verk på sin egen digitala mojäng, om det sker för eget bruk. Användaren kan också t.ex. lyssna på denna musik via högtalare i sin egen apparat, men man får inte framföra musiken offentligt och inte heller eljest göra den tillgänglig för allmänheten, om upphovsmannen inte har gett sitt samtycke därtill.

De upphovsrättsliga problemen börjar, då man sparar verk på servern eller annan tjänst utan upphovsmannens tillstånd. I praktiken betydelsefulla typexempel berör de situationer, då det olovligen sparats filer innehållande musik, film eller andra verk t.ex. för att kopieras av allmänheten. Det är klart, att spararen av filen har då olovligen framställt exemplar av verk. Länkläggaren åstadkommer inte själv framförande eller framställning av verksexemplar, om Internet-användaren själv hamnar att trycka på knappen för att sätta i gång framförandet eller annars separat via kopieringskommando utföra en kopiering av filerna. Länkläggaren kan vara medveten om, att filerna har olovligen kopierats. Om en Internet-användare får olovliga filer till sitt bruk via länkar och om han använder filerna ett sådant sätt, att de kränker de ekonomiska rättigheter, som tillhör verkets upphovsman, är det klart, att länkläggaren är en medhjälpare eller anstiftare till Internet-användarens

upphovsrättsliga brott. Länkläggarens delaktighet avgörs i enlighet med vederbörandes förhållanden. Det är å andra sidan givet att exploateringen av verk i digital miljö också medfört att man kan fråga sig hur användaren skall veta om ett verk lagligen har spridits i nätverk. Följdriktigen framstår då frågan om användarens ansvar för länkning till olovliga verk. Exempelvis i amerikanska fallet *DVD Copy Control Association v. Andrew Bunner*, 113 Cal.Rptr.2d 338, 2001 hade vanliga länkar till DVD-krypteringskod publicerats. Domstolen ansåg att den som uppehåller en lista över vanliga länkar inte kan anses ha ansvar för innehållet på de sidor som man länkar till, emedan det däremot borde vara innehavarna av webbsidorna, som bär ansvar för tillgängliggörande av olovligt material.

Hämtande länkar

Då man vid hämtande länkning integrerar text, bild, ljud eller multimedia, antingen med eller utan ramar, sker förutom ett tillgängliggörande för allmänheten dessutom ofta en exemplarfram-ställning hos utnyttjaren. Detta med anledning av, att varje gång utnyttjaren öppnar en webbsida hos länkläggaren, sker ett framförande av verk och han får bl.a. en kopia av webbsidan och bilder på sin digitala mojäng.

Då länkläggaren lägger ut en hämtande länk för att användaren vid ankomsten till länkläggarens sida obönhörligen skall ta del av upphovsrättsligt skyddat material, kan man tala om ett utnyttjande av verk, vilket innebär att olovlig användning gör intrång på upphovsmannens förfoganderätt enligt 2 § URL. Bilder visas, medan musikaliska verk framförs. För att länkläggaren överhuvudtaget ska ha kunnat skapa en webbsida, har exemplar av verk framställts.

Dels utgår man ifrån att hypertextfilen lokalt finns på länkläggarens eget serverutrymme, fast eller löst, t.ex. uppe bland molnen, dvs. den som har skapat utrymmet (webbsidan), framställer exemplar av upphovsrättsligt skyddade verk, som nås via filen, vilket innebär att exemplar framställs vid länkläggarens anlitade utrymme, då upphovsrättsligt skyddade verk efterfrågas av användarna.⁵ Dels kan hypertextfilen finnas på någon annans fasta eller lösa utrymme och länk-läggaren har bara en hämtande länk på sin webbsida, varmed upphovsrättsligt skyddade verk kan sökas och exemplar framställas någon annanstans, innan det efterfrågade materialet sänds till utnyttjaren. De upphovsrättsligt skyddade verken (text, ljud, bild eller multimedia) har också tillgängliggjorts av länkläggaren för allmänheten i enlighet med 2 § URL.

En hämtande länk kan hämta till ett annat fast eller löst utrymme exempelvis en sparad musikfil, som spelas automatiskt upp som bakgrundsmusik, då användaren kommer till länkläggarens webbsida. De upphovsrättsliga tolkningsproblemen börjar, om länkläggaren inte har erhållit samtycke av det musikaliska verkets upphovsman att framföra bakgrundsmusiken. Tekniskt sett hämtar användarens webbläsare musikfilen från ifrågavarande nätverksutrymme och framför det musikaliska verket via mojängens högtalare. Det föreligger inget skäl att behandla situationen så, att länkläggarens och användarens handling tas separat till behandling. Ett dylikt granskningssätt skulle betyda, att man skulle glömma bort helheten.

Vid en jämförelse med andra rättsområden i Finland har man t.ex. vid skatte- och ekonomiska brott för vana att behandla rättsinkräktarens verksamhet som en helhet. Med andra ord ser man separat utförda handlingar som en helhet eller seriehandlingar.⁶ Om man betraktar varje handling åtskilt och självständigt i förhållande till andra handlingar, så kan varje handling ensam verka laglig. Situationen kan verka helt annorlunda, om handlingar som utförts i en följd ses som en helhet då man beaktar de syften och mål som hänför sig till rättsinkräktaren. För en hämtande länk innebär det, länkläggarens handlingar inte bör säras från de handlingar och följder, som Internet-användaren utför och förorsakar på basen av länkläggarens programmering. Länkläggaren av en hämtande länk

⁵ Se Sanger 1996: 2.

⁶ Se om seriehandlingar närmare i t.ex. Tikka & Nykänen 2000: 14–15.

vet, att användarens webbläsare hämtar t.ex. musikfilen från en annan server, fast eller lös, och att det musikaliska verket framförs hos användaren via högtalare. Detta sker just med anledning av länkläggarens programmering. Internet-användaren vet inte nödvändigtvis, att olovlig bakgrundsmusik framförs automatiskt, då han godtroget kommer till länkläggarens webbsida. Länkläggaren använder en utomstående Internetanvändare och hans webbläsare som en mellanhand för att framföra litterära och konstnärliga verk hos användaren. Länkläggaren har uttryckligen avsett detta. Frågan gäller inte summan av tillfälligheter, utan det är fråga om ett resultat av en målinriktad verksamhet. Detta framförande är offentligt, eftersom verket har tillgängliggjorts för en på förhand individuellt obestämd personkrets.

Problematiskt i sammanhanget är, att författare har oftast glömt bort att specificera vilken typ av cache de hänvisar till. Således blir diskussionen beträffande cache ganska vag.⁷ Åsikter framförs bland ett antal författare, att det är i användarens digitala apparat som en kopiering sker i cache-filen.

Däremot är ett flertal författare i stort sett ense om, att ingen exemplarframställning sker hos länkläggaren. Påståendena gäller bl.a., att det inte framställs exemplar, varken då länken skrivs in i HTML-koden eller då materialet hämtas. Uttalandena rör sig rätt och slätt om att någon kopia inte görs på cache-filen hos värdservern. Man konstaterar också, att den som skapar den hämtande länken, inte kopierar de verk som finns på den sida som länken går till.

Här framhävs däremot, att eftersom exemplaret eller verket kopieras med hämtande länk på användarnas dator eller annan digital mojäng, innebär det att länkläggaren med tillhjälp av den hämtande länken har framställt exemplar av verket, då länken lagts ut och då den hämtas automatiskt av användarnas webbläsare. Detta medför också att länkläggaren då tillhandahåller verktyg, dvs. automatiskt bereder tillgång till aktuellt material genom den hämtande länken.

Frågan kan också få upphovsrättslig aktualitet i annat sammanhang, eftersom upphovsmannen kan appellera till sin ensamrätt enligt 2 § URL då man använder, dvs. förutom framställer exemplar, också gör verksexemplaren tillgängliga för allmänheten utan tillstånd.

Ytterligare kan man konstatera, att användaren inte heller kan vara medveten om att det är upphovsrättsligt skyddade verk som kopieras i hans digitala mojäng då han via länkläggaren automatiskt får tillgång till material, och inte heller att det sker olovligt.

Man kan notera olägenheten med länkar också från andra perspektiv. Dels genom att den hämtande länken kan vara uppbyggd så, att den laddar filer i en skild ram (frame), vilken ändå visar sig för användaren såsom en del av en annan sida, vilket kan vilseleda användaren. Det kan således gälla a) olovliga filer eller b) att innehavaren av webbsidan inte önskar ha länkar till filerna i fråga. Dels kan särskilt ur marknadsföringssynvinkel nackdelen medföra att de vanliga länkarna är s.k. djuplänkar och leder användaren till s.k. subsidor. Djuplänken går förbi portaler eller ingångssidor, som innehåller marknadsföringsprospekt, som man önskar att besökare tar del av. T.ex. i fallet Bundesgerichtshof 17.7.2003, I ZR 259/00 (*Paperboy*) hade i nyhetssöktjänsten satts djuplänkar till olika nyhetsartiklar. Enligt domstolen utgjorde djuplänken en vanlig länk och konstituerade därmed inte upphovsrättsintrång, trots att användningen av sökmaskiner kan minska innehavarens reklamintäkter. I målet Bundesgerichtshof den 29.4.2010, I ZR 39/08 (*Internetkartor*), där en länkläggare i egenskap av näringsidkare satt djuplänk direkt till ett företags sida, där man saluförde en specifik lägenhet, ansågs länkläggaren ha gjort intrång i rätten till tillgängliggörande. Problemet var, att privatpersoner kunde använda tjänsten ifråga gratis, medan kommersiella utövare skulle skaffa licens för utnyttjandet och för att kunna länka till portalen.

⁷ Se närmare bl.a. Rahnasto 1998: 98–99 och Carlén-Wendels 2000: 176. Se däremot Lehtonen 2005: 994 och Sorvari 2007: 79, 126.

4. Tillgängliggörande för allmänheten

Upphovsrättsrådets utlåtande 2001: 8 föranleder att diskutera begreppet tillgängliggörande för allmänheten i länksammanhang, med anledning av den vaga tolkningen av länkproblematiken.

Emedan ett rättsfall som slutade i förlikning inte ger tillgång till tingsrättens domskäl bör man förlika sig på Upphovsrättsrådets utlåtande, där man tog ställning till att länken var en hämtande integrerande länk.

UR 2001:8. Redaktören Sirpa Norri som arbetat som free lance-redaktör och skrivit medicinska artiklar till A-lehdet Oy, vilka publicerats i tidskriften Kauneus och terveys. A-lehdet Oy hade utan Sirpa Norris vetskap lagt ut på tidskriften Kauneus ja terveys' webbsida med fri tillgång till att läsa 21 artiklar som hon skrivit under perioden 27.3.1996–12.11.1999. Detta förfarande kunde göras med anledning av att det i avtalet stod inskrivet om återanvändningsrätt.

Sedermera hade A-lehdet Oy ingått ett samarbets- och marknadsföringsavtal med MediXine Oy. Enligt detta avtal hade A-lehdet Oy mot ersättning fått göra reklam för tidskriften Kauneus och terveys på MediXine Oy:s webbsida sk. Nätklinik (Verkkoklinikka) och å sin sida hade MediXine Oy fått lägga länkar från sina webbsidor till tidskriften Kauneus och terveys' sidor och material. MediXine Oy hade länkat till 5 av Sirpa Norris artiklar under tiden 13.1.1998–8.11.1999.

Man hade på basen av de av Sirpa Norris artiklar, som utnyttjats, gjort på MediXine Oy:s webbsidor en Avink@ som behandlade ämnet i artikeln. I Avinken@ hade man nämnt Sirpa Norris namn, men däremot inte att materialet stod att finnas bland tidskriften Kauneus och terveys' material. Användaren kunde därmed få den uppfattningen att Sirpa Norri skrivit för MediXine Oy och överlåtit upphovsrätten till denne. MediXine Oy är inte ett journalistiskt forum.

Från Sirpa Norris artiklar hade gjorts en Avink@ som behandlar ämnet i artikeln på MediXine Oy:s webbsidor. Under vinken hade funnits en länk till Sirpa Norris artiklar. Både vinken och länken hade funnits på MediXine Oy:s webbsidor (Nätkliniken Verkkoklinikka) under adressen: www.verkkoklinikka.fi/. Länken hade fört användaren till Sirpa Norris artiklar. MediXine Oy hade hela tiden kvarstått som webbadress. Sirpa Norris artiklar hade således kunnat läsas från MediXine Oy:s webbsidor och den länkade sidans webbadress hade inte kommit till synes. Däremot hade nog tidskriften Kauneus och terveys' reklam funnits på samma sida eller i början av artikeln.

Upphovsrättsrådet ansåg att denna hämtande länk gjorde intrång på upphovsmannen Sirpa Norris verk, artiklar, i enlighet med 2 § 3 mom. URL. De upphovsrättsligt skyddade verken mångfaldigades och tillgängliggjordes för allmänheten och i detta hänseende för en ny publik utan upphovsmannens tillstånd. Härmed kan man anse att länkläggandet var en upphovsrättsligt relevant handling, som tillhör sfären för upphovsmannens ensamrätt.

Upphovsrättsrådet gav också i sitt utlåtande uttryck för att en ordagrann och snäv tolkning av 2 § 3 mom. URL måhända inte skulle kunna anses för ett tillgängliggörande för allmänheten. Jag anser däremot att denna länkning gällde just en hämtande integrerande länk och ett tillgängliggörande för allmänheten då man framförde de skyddade verken, artiklarna, och URL-adressen inte ändrades till tidskriften Kauneus och terveys' webbadress, vilket skulle ha inneburit att användaren helt förflyttades till målsidan.

Rättsfallet berörde ytterligare en synnerligen relevant fråga: Sirpa Norris artiklar hade publicerats i tidskriften Kauneus och terveys. A-lehdet hade därefter fört artiklarna till den egna webbsidan. A-lehdet ansåg att frågan om att A-lehdet placerat artiklarna på webbsidan baserade sig på ett avtal mellan A-lehdet och Sirpa Norri. A-lehdet och MediXine Oy hade sedermera uppgjort ett avtal enligt vilket MediXine Oy hade lagt länkar till A-lehdet och Sirpa Norris artiklar. MediXine Oy ansåg att fastän länkningen var upphovsrättsligt relevant hade Sirpa Norri gett sitt tillstånd till det med anledning av sitt avtal med A-lehdet.

Enligt 28 § URL må, om ej annat avtalats, den till vilken upphovsrätt överlåtits, ej överlåta rätten vidare. A-lehdet hade inte tillstånd att överlåta den upphovsrätt som erhållits genom avtalet med Sirpa Norri vidare till MediXine Oy, om inte därom avtalats.

Enligt de traditionella upphovsrättsliga lagreglerna har upphovsmannen en uteslutande rätt att på två sätt förfoga över verket. Ensamrätten är inte generell. Förfoganderätten gäller enligt 2 § 1 mom. URL a) att framställa exemplar av verket och b) att göra det tillgängligt för allmänheten. Paragrafens 3 mom. ger exempel på olika sätt att göra ett verk tillgängligt för allmänheten. I rättspraxis har småningom etablerats en vedertagen bedömning av överföringens rättsliga natur.

Om ett verk eller annat material överförs till allmänheten eller tillgängliggörs för allmänheten i elektronisk form, uppstår ett exemplar av det skyddade materialet i arbetsminnet eller på hårddisken i användarens dator eller på ett liknande upptagningsunderlag. Det är möjligt att användaren av ett sådant upptaget exemplar framställer även en utskrift eller en kopia på ett separat fysiskt underlag. Ett sådant exemplar av ett material inte spridas vidare. Således förutsätts alltid rättsinnehavarens tillstånd för att sprida ett fysiskt exemplar av ett verk som levererats via en online-tjänst. Tillståndet kan vid behov tas in i villkoren för onlineleveransen. Konsumtionen av rättigheter hänför sig inte i något skede av distributionskedjan till "immateriella" tjänster.

Framföranderätten hör till en av upphovsmannens uteslutande rättigheter att göra verket tillgängligt för allmänheten i enlighet med 2 § 3 mom. URL. Tillgängliggörandet för allmänheten kan innebära ett offentligt framförande som sker genom att a) direkt eller b) indirekt återge verket.

Betydelsefullt för framföranderätten är bestämmandet av när verket tillgängliggjorts för allmänheten, såväl i traditionell som via ny teknik. Verket har gjorts tillgängligt för allmänheten då det framförs offentligt. Offentlighetsrekvisitet har inte noggrannare definierats i lagen. Det blir därför erforderligt att göra en gränsdragning.

Överlag må man ponera huruvida den ensamrätt som tilldelats upphovsmannen enligt 1 momentet är täckande i digitala kommunikationsnätverk och om förteckningen i 3 momentet är endast ett exempel på de förfoganden som tillhör upphovsmannen och sålunda omfattar otaliga former av tillgängliggöranden, eller innefattas i momentet endast de former av tillgängliggöranden som exemplifieras i momentet? Enligt kommittébetänkandet har man endast åskådliggjort olika former att tillgängliggöra verket för allmänheten. De facto kan man tolka lagregeln i 3 momentet som entydig och klar och inte en exemplifiering.

5. Reklam på portalsidan

Bör länken göras till ett annat företags ingångs- eller hemsida (portal), där det finns reklam som ger intäkter, eller kan man leda användaren med länk förbi ingångssidan direkt till underregister eller -sida (djuplänk, deep link). En vanlig länk kan i princip läggas förbi portalsidan, men om reklamföreteelser kan anföras bl.a. att enligt 1 § konsumentskyddslagen är stadgat om förbud i fråga om marknadsföring som strider mot god sed och otillbörliga förfaranden. Enligt paragrafen får marknadsföringen inte strida mot god sed och vid marknadsföring får det inte tillämpas förfaranden som är otillbörliga mot konsumenterna. I detta sammanhang kan av ovan sagda anföras att, t.ex. användning av domännamn, såsom länkning till en webbsida med pornografiskt innehåll är inte godtagbart och således inte enligt god sed. Ett förfarande har aktualiserats i ett antal fall, bl.a. *CCA Industries, Inc. v. Bobby R. Dailey*, (Nr D2000-148) där käranden i sitt käromål hade poängterade den skada han skulle lida med anledning av att varumärket "bikini zone" genom svarandens domännamnsregistrering "www.bikinizone.com" länkades till en pornografisk webbsida. Misstankar därom i fallet *Nokia Corporation v. Nokiagirls.com*. a.k.a. IBCC (Nr D2000-0102)40).

Med otillbörliga förfaranden avses sådana olämpliga förfaranden som sannolikt kommer att påverka konsumentens ekonomiska beslutsfattande. Med marknadsföring avses kommersiella meddelanden, såsom reklam, information som i samband med olika säljfrämjande åtgärder.

Om ansvarsfrågan, då det gäller verksamheter i nätmiljö, inte endast berör upphovsrätt och närstående rättigheter utan även andra områden, t.ex. förtal, vilseledande reklam och varumärkesintrång, behandlas denna fråga på ett övergripande sätt i direktivet om elektronisk handel, som förtydligar och harmoniserar olika rättsliga frågor i samband med informationssamhällets tjänster, bl.a. elektronisk handel. Exempelvis en hämtande länk till skyddade verk och samtidigt skyddade varumärken, såsom sloganer, kan konstituera intrång, särskilt om det sker i näringsverksamhet. Uttrycket "kaikki on vinksin vonksin tai ainakin heikun keikun" åtnjuter enligt upphovsrättsrådets utlåtande 2010: 2 upphovsrättsligt skydd och kunde förslagsvis bli föremål för utnyttjande p.g.a. det humoristiska uttryckssättet.

I tillämpningsöversikten till E-handelsdirektivet KOM(2003) 702 s. 250 beskrivs det tyska fallet om länkar, BGH den 17.7.2003, mål I ZR 259/00 (*Paperboy*). Den vanliga länken var en hänvisning till och information om upphovsrättsligt skyddade verk och utgjorde inte intrång i upphovsmannens ensamrätt till exemplarframställning eller tillgängliggörande. Enligt domstolen stred läggande av den vanliga länken inte mot god marknadsföringssed. De förenade målen i EU-domstolen, *Google France SARL och Google Inc. v. Louis Vuitton Malletier SA*, C-236/08 och *Google France SARL v. Viaticum SA och Luteciel SARL*, C-237/08, gällde Googles användning av nyckelord eller adwords i sitt hänvisningssystem. Google ansågs inte använda dessa varumärken i sin egen kommersiella kommunikation. Däremot betonar domstolen i mål *L'Oréal v. eBay*, C-324/09, att undantaget i artikel 14.1. direktivet om elektronisk handel inte gäller för en tjänsteleverantör om denna utövar en aktiv roll genom att bistå med hjälp, såsom att optimera marknadsföringen av aktuella erbjudanden. T.ex. i Finland har finska musikbolag bett Google ta bort 10.000-tals länkar.

Ytterligare kan poneras om att reklam i näringsverksamhet inte får användas förfarande, som strider mot god affärssed eller eljest är otillbörligt mot annan näringsidkare enligt 1 § Lag om otillbörligt förfarande i näringsverksamhet. T.ex. i det tyska fallet *Landgericht Hamburg*, 2.1.2001, 312 O 606/00 ansågs länkning utgöra UWG (*Gesetz gegen den unlauteren Wettbewerb*, 3.7.2004, BGBl. 1. S. 1414) och stridande mot 1 §. Fråga i fallet var, att länkläggaren hade satt en vanlig länk till konkurrerande företags sidor på så sätt att användaren kunde vilseledas att tro, att länkläggaren och kändanden hade ekonomiska relationer. Kritik kan anföras, emedan en vanlig länk torde inte medföra otillbörlighet

Däremot innebär kommande licensavtal mellan *Youtube* och *Teosto* att utövande konstnärer och upphovsmän får reklamintäkter.

6. Förmedlande av nyheter

Utländska konflikter beträffande länkar blev ett uppmärksammat ärende då det gäller *Total News*, dvs. en sida, vilken specialiserat sig på förmedlande av nyheter. *Total News* hade inte själv producerat eget material, utan tillhandahållit länkar till en stor mängd nyhetssidor. Andras material hade hämtats till ramar, för att presenteras i samband med *Total News'* meny och reklam. Ett flertal tidskrifter t.ex. *Washington Post*, *Time/Life*, *CNN*, *LA Times*, *Dow Jones* och *Reuter* väckte åtal p.g.a. ramtekniken. Utöver andra olagligheter, gällde de upphovsrättsliga intrången olovlig exemplarframställning och tillgängliggörande för allmänheten. Till *Total News'* webbsidor hade hämtats främmande webbsidors material till en ram, vilket utgör ett upphovsrättsligt intrång enligt 2 § URL, eftersom upphovsmannen har en uteslutande rätt att förfoga över verket genom att framställa exemplar därav. Det främmande materialet gjordes tillgängligt för allmänheten genom att „återutsända“ materialet.

De stora nyhetstidskrifternas intresse för nyhetsvärdet gällde främst de investeringar som gjorts i nyhetsmaterialens tillkomst och publicering. Total News undgick helt dessa kostnader, och kunde dessutom få intäkter från reklamutrymmena på sin sida. Det skedde en förlikning parterna emellan, under förutsättning att Total News inte visar material från någon kändepart, endast på en del av bildskärmen, samt att länken bör vara en vanlig länk.

Den vanliga länken innebär att användaren förflyttas helt bort från Total News' sida. Detta innebär att användaren förflyttas till måldokumentet, som kan vara någon av de berörda nyhetstidskrifternas sida. Då har Total News endast hänvisat användaren till annan sida och inte förorsakat någon exemplarframställning.

Att Total News var tvungen att använda hela sidan i stället för endast en del därav, kan tolkas som att kändeparten önskar förhindra, att extra reklam smygs in bland de ytterst förmånliga nyhets-sidorna.

Exempelvis i fallet Cour d'appel de Bruxelles, 5.5.2011, *Copiepresse v. Google* hävdade svaranden med hänvisning till yttrandefriheten, att de har rätt att utnyttja annans upphovsrätligt skyddade material i sin nyhetstjänst.⁸ Fråga var inte om egentliga länkar, utan s.k. kardborrar, som var programmerade att automatiskt söka efter nyhetsmaterial och således inte exempelvis en fysisk persons agerande, vilket också värderades i bedömningen. Svaranden framställde enligt domstolen exemplar av kändes material och överförde det till allmänheten, trots att fråga var om cache-minnet.

Ett annat fall gällde The Shetland News, vilken hade dels eget material, dels länkar till nyhetsartiklar vid andra tidskrifter, däribland Shetland Times. Länkarna var vanliga, förflyttande länkar, vilka hade en länktext, som bestod av respektive artikels rubrik. Användaren förflyttades direkt till den eftersökta artikeln. På så sätt undgick all reklam exponering för användarna på Shetland Times' ingångssida (portalsida). I uppgörelsen förutsattes bl.a. att det under rubriken anges a Shetland Times Story och att länkarna skall leda till Shetland Times' ingångssida och inte direkt till artikeln i fråga.

The Shetland News ansågs olovligen ha framställt exemplar av Shetland Times rubriker, då Shetland News lagt in rubriken i själva länken. Upphovsmannens uteslutande rätt att förfoga över verket eller delar därav har kränkts enligt 2 § URL genom att The Shetland News utnyttjat Shetland Times' rubriktexter som länkmärke. Om man appellerar till citaträtten enligt 22 § URL, bör man beakta huruvida citering sker i marknadsföringssyfte samt beaktande av appelleringssituationen och omfattningen av citatet. Överlag anses sådan citering inte godtagbar, men då skall helst det gemensamma syftet ifrågasättas. I rättsfallet gjorde man citeringen egentligen inte för egen vinnings skull, utan man önskade helt enkelt med den förflyttande vanliga länken, hänvisa till annat material. Dessvärre förflyttades användaren direkt till sidan ifråga, vilket innebar att reklamsidan hos måldokumentet Shetland Times inte fick besökare. Kommersiella intressen har fått en allt större tyngd vid länkfrågor.

Följande rättsfall, som väckte mycket uppmärksamhet belyser problematiken i Norden:

Ett domslut i Skövde tingsrätt gällde yrkande, som baserar sig på antagandet om brott mot upphovsrättslagen. Enligt åtalet hade A under tiden hösten 1998 till juli 1999, i sin bostad i Stenstorp, genom att framställa eller kopiera, eller i varje fall sprida olagliga ljudfiler i MP3-format från CD-skivor och göra dem tillgängliga via sin egen webbsida på Internet, uppsåtligen eller av grov oakt-samhet, vidtagit åtgärder varigenom han gjort intrång i de rättigheter som tillkommer de skilda skiv-bolagen – totalt 53 st – genom deras företrädare Ifpi.

⁸ Se även om yttrandefrihet Still 2007: 168–169.

Här granskas A:s agerande: A hade, på sin webbsida, levererat information som hänför sig till musiktitlar, länksymboler etc. Detta hade A gjort i avsikt att göra musikfilerna tillgängliga, för att ladda ner musikfiler från externa servrar. Filerna hade i sin tur sparats från CD-skivor. A länkade informationen genom vanliga länkar till olika servrar, där de musikaliska verken var sparade såsom musikfiler. Detta möjliggjordes för användare, som besökte A:s webbsida, enbart genom att klicka en gång på webbsidans länkbeteckning, utan att slinka in på någon annans webbsida, för att erhålla filerna direkt till sina datorer, utan mellanlandning hos A. Länkarna medförde att användaren inte själv behövde söka efter adresser varifrån filer kan laddas ner. Användarna kunde via A:s länkar komma åt musikfilerna. Detta i den mån A:s handlande var nödvändigt för exemplarframställning av en kopia i de datorer, som utnyttjat A:s erbjudande om länkarna. A hade förstått att musikfilerna var olagliga, men kunde inte föreställa sig att länkarna var det.

Om man är medveten om att upphovsrättsliga intrång görs, med anledning av marknadsföring av länkar till andra webbsidor, bör man se till att frågan om gällande medhjälp till 1) olovlig exemplarframställning och 2) tillgängliggörande för allmänheten blir aktuell. Relevant i sammanhanget är, huruvida användarnas exemplarframställning sker för annat ändamål än enskilt bruk, vilket är tillåtet enligt 12 § URL, eller huruvida den medhjälpande parten dessutom erhåller ekonomisk ersättning för sin delaktighet. Det är tillåtet att själv framställa enstaka exemplar av offentliggjorda musikaliska verk för eget bruk, enligt 12 § i de nordiska upphovsrättslagarna. Enligt 12 § 3 mom. URL får inte framställning av exemplar av musikaliska verk för uppdragsgivarens enskilda bruk ges åt utomstående. Man kan anse, att även andra, förutom de användare som besökte A:s webbsida, tog del av exemplarframställningsprocessen. MP3-filerna tillhandahölls inte av användarna, utan av assistans av de personer, som hade lagrat musikfiler och bytt ut icke-fungerande länkar på servrarna.

Man kan också ifrågasätta A:s delaktighet genom användarnas kopiering av musikfiler. Tingsrätten ansåg att det inte hade bevisats att användarna hade kopierat musikfilerna för något annat ändamål än för eget bruk.

I ifrågavarande rättsfall var exemplaren offentliggjorda, men man kan anse att den som ställt exemplaren till förfogande på nätet, begått ett upphovsrättsligt intrång, eftersom handlingen var olovlig. Vid beaktande av stadgandena om inskränkningarna i 2 kapitlet, torde däremot förlagan (mastern) eller dess kopia endast vara tillämplig, om förlagan (mastern) i sig själv är ett lagligt exemplar. Enligt 12 § URL bör verksexemplaret vara offentliggjort, vilket innebär att man inte får kopiera för sitt enskilda bruk av icke-offentliggjorda verksexemplar. Detta förbud gäller också, ifall man kopierar av verk, som nog offentliggjorts, men utan tillstånd av rättsinnehavaren. I enlighet med detta kan man anse att piratkopior o.a. olagliga exemplar av ett upphovsrättsligt skyddat verk inte kan skyddas av inskränkningarna i upphovsrätten enligt 2 kapitlet. Inte förrän upphovsmannen har utgivit, publicerat eller överfört sitt verk eller kopior av det, kan andra beviljas en säker rätt att använda verket utan speciellt tillstånd.

Ett aktuellt problem i dylika sammanhang är, då en hänvisning kan betraktas som ett tillgängliggörande för allmänheten. Förutom a) framförandet beaktas tillgängliggörande i bemärkelsen b) utbjuda till försäljning eller eljest c) sprida.⁹

Hänvisande till ovanstående rättsfall beaktas följande:

a) Man kan vid närmare granskning se, att varje digitala kopia av en musikfil, som ligger på någon fast eller lös server, och till vilken A hade uppgjort länkar, kan de facto representera en anordning, på vilken ljud har tagits upp och kan återges. A hade m.a.o. medverkat till att göra dessa lättill-

⁹ Se även Rosén 2000: 8–14.

gängliga för allmänheten genom hänvisning via de vanliga länkarna till webbsidor i Internet, där man kan finna MP3-filer. Detta för att allmänheten inte själv behövde söka efter källan.

b) A hade haft många besökare på sin webbsida, men inte ännu förtjänat pengar på sin verksamhet, även om han haft förhoppning om att göra det. Man kan m.a.o. anse att domstolarna vägde de ekonomiska aspekterna lätt i sammanhanget, eftersom A:s avsikt med länkningen var ett agerande i förvärvssyfte, då ett företag dessutom marknadsförde sig via hans webbsida.

c) Problemen vid upphovsrättsliga intrång i öppna kommunikationsnätverk i samband med länkning har till stor del också berört informationen om verket. En klarläggning beträffande information delvis ur marknadsföringssynvinkel stöder argumenteringen kring informationens betydelse i sammanhanget. Ur den marknadsförande partens sida är en av de huvudsakliga kriterierna för verkets avsättning att information ges om verket i fråga.

För att verket skall finna sin väg till användaren bör denne informeras om dess existens. Någon konflikt mellan intresset att informera om verk och intresset att skydda rättsinnehavarens upphovsrättsligt skyddade verk borde i grunden egentligen inte finnas.

Här understrykes betydelsen av kommunikation också i detta sammanhang. I ovanstående rättsfall kan man å ena sidan appellera till information och kunskaper, dvs. att utnyttjarna också bör inneha stor datorvana, för att inse att MP3-filen inte legat på samma ställe (server) som A:s webbsida. Här anses kommunikationen dessutom motsvara den tekniska funktionen, då man följer användarens agerande efter informationshämtningen. Å andra sidan kan man se, hur i berörda rättsfall A ansåg, att orsaken till att han haft så många länkar till sin webbsida, hade varit att önskan att ha många besök på den, så att säga få till stånd interaktiv kommunikation.

Slutligen kan anses, att A har bidragit till att musik kopierats från servern till användarnas datorer. Väsentligt i sammanhanget är, huruvida A vidtagit åtgärder för att göra det möjligt för allmänheten att få tillgång till upphovsrättsligt skyddade musikaliska verk. Fastän musikfilerna inte fysiskt passerade A:s webbsida, fanns kommandot på webbsidan såsom ett instrument och startpunkt. Rätten att framställa exemplar av verket hör onekligen till upphovsmannens ensamrätt.

Länkarna har allt mer blivit en väsentlig del av marknadsföringsprocessen i Internet. För att erhålla förståelse för affärsverksamheten i elektroniska medier och dess tillväxtmöjligheter där, krävs att man också ser sambanden mellan upphovsrättsliga frågor och påverkande marknadsföringskriterier. Informationens, kommunikationens och den för länkarnas vidkommanden särpräglade interaktionens betydelse kan inte underskattas. Upphovsrättsliga intrång uppstår inte ur intet. Utnyttjarna har informerats om verken, de kommunicerar och det interaktiva förhållandet uppkommer. Därom vittnar den mångfaldiga nättaktiviteten.

7. Avslutande kommentarer

Sådana intrång i upphovsrätten som sker inom nätverk och med hjälp av datasystem har formats till ett problem av t.o.m. ännu större omfattning än försäljningen av piratkopior av ljud- och bildupptagningar.

Det synes som att tekniken i utnyttjandet av de serverlösa nätverken fick sin början, men noteringen av dem hinner inte i takt med de tekniska tilltagen. De s.k. serverlösa nätverkstjänsterna med tillkomsten av Napster-tjänsten möjliggjorde ofantliga intrång i upphovsrätten. Man uppskattade, att enbart inom dessa tjänster omfattade den olovliga distributionen närmare en miljard filer. Den „äkta“ P2P varianten i Gnutella-systemet var även aktuell. Sedermera utvecklades Aimster och Grokster (FastTrack nätverk) samt KaZaA med ca 5 ca miljarder filer och har varit ett av de största serverlösa nätverken. KaZaAs fildelningsprogram var tidigare också ett av de mest nedladdade programmet på Internet. Otillåten fildelning via fildelningsajten *The Pirate Bay* fick ett enormt mass-

medialt pådrag, med den s.k. BitTorrent-tekniken. I Finland har högsta domstolen avgjort mål, där fråga var om fildelningsnätet Finreactor och uppladdning skedde med s.k. torrentfiler, HD 2010:47 och 2010:48. I fallen hade svaranden gjort intrång i rättsinnehavarnas rätt att tillgängliggöra verk för allmänheten i enlighet med 2 § 3 mom. URL.

Aktuella tekniker har även inom nyhetsförmedling varit den s.k. crawling-tekniken, RSS-in-matningstekniken och kardborrstekniken, som fäster och förenar enligt inmatade kommandon.

Dessa är inte länkar i ursprunglig mening utan snarare oauktoriserade operationer för utnyttjande av skyddade verk i stor skala. Å andra sidan skall de beskrivna tekniska lösningarna inte vara avgörande, emedan man skall för den upphovsrättsliga helhetsbedömningen se till sluteffekten.

8. Summary

One of the problematic phenomena of the open network in recent decades from a copyright point of view has been the illegal distribution of musical works and cinematographic works.

In Finland, the prevailing conception has been that by placing a website on a server to be accessible to the general public without restrictions, the author has given his or her consent to normal use of the site. This conception seems to be justified. Normal use of a website includes a right on the part of users to freely access the site and skim through, look at and read pages and, by extension, to print material out on paper for their own use. Normal use also allows the author of a site to place restrictions on access if he or she does not permit it to be freely used. This can happen via user names, passwords, and technical or other restrictions, as mentioned in Bundesgerichtshof 19.10.2011, I ZR 140/10 (Vorschaubilder II), Bundesgerichtshof 17.7.2003, case IZR 259/00 (Paperboy) and Bundesgerichtshof 29.4.2010, case I ZR 69/08 (Google).

The problems from a copyright point of view begin when a work is saved on a server or other service without the consent of the author. In practice, examples of such situations are when files containing music, films and other works are saved and then copied by the general public. It is clear that the person saving the file has illegally produced a copy of the work.

A person who has made a link available does not produce a copy of a work if the Internet user has to push the button to start the performance or to use some other command to copy the file. The one who has provided link may be aware that the files are illegally copied. If an Internet user gets access to illegal files via links and if he or she uses the files in a way that infringes the economic rights of the author of the work, it is evident that the person providing the link has abetted or instigated a copyright infringement by the Internet user. The former's complicity is determined according to the circumstances. On the other hand, it is a given that the exploitation of works in the digital environment makes it justifiable to ask how the user is to know whether a work has been legally distributed on networks. Here the focal question becomes the responsibility of the one who has provided the link. For example, in the American case DVD Copy Control Association v. Andrew Bunner, 113 Cal.RPtr.2d 338, 2001, normal links to a DVD decrypting code had been published. The court was of the view that a person who maintains a list of normal links cannot be held responsible for the content of the sites to which the links lead; it should be the owners of the websites who are held responsible for making illegal material accessible.

Collecting, linking and integrating text, pictures, sounds or multimedia, with or without frames, is an instance of making material accessible to the public and of the user making a copy of it. Thus, every time a user opens a website, a performance of the work occurs and the user gets a copy of the website and pictures on his or her digital device.

A link may redirect to a file with music that is automatically played as background music when the user accesses a website. The problems from a copyright point of view begin if the person who has

provided the link does not have the consent of the author of the musical work to perform the background music. Technically, the web reader collects the file of music from the network space in question and performs it through the loudspeakers of the digital device. There are no reasons to separate the acts of the person who has provided the link and the user when considering such a case; one would lose sight of the situation as a whole.

Copyright infringements on networks and using computer systems have even become a larger problem than the sale of pirate copies of sound and picture recordings.

It appears that the technique originated with the use of serverless services, but the attention these received did not keep pace with the technical development. The so-called serverless network services, such as Napster, made substantial copyright infringements possible. It is estimated that the number of illegal files within these services was as high as 1 billion. The Gnutella system also involved a real P2P variant. Then Aimster and Grokster (FastTrack network) were developed, as well as KaZaA, which has about 5 billion files, making it one of the largest serverless networks. The KaZaA's file-sharing program has been the one of the most frequently downloaded programs on the Internet. The illegal file sharing through the site The Pirate Bay using BitTorrent technology received enormous publicity in the mass media.

In Finland the Supreme Court handed down a decision in a case involving the file-sharing network Finreactor and uploading using so-called torrent files, HD 2010:47 and 2010:48. In the cases the defendants infringed the right holders' right to make works accessible to the public as set out in section 2, subsection 3 of the Copyright Act.

Other techniques have also been topical, such as crawling and RSS. These are not normal links but unauthorized operations for use of protected works on a large scale. On the other hand, it is not the technical solutions that are decisive; rather, one has to look at the final result to arrive at a consistent assessment from point of view of copyright.

9. References

Carlén-Wendels, Thomas (2000). Nätjuridik. Lag och rätt på Internet. Tredje upplagan. Stockholm: Norstedts Juridik AB.

Europaparlamentets och rådets direktiv 2001/29/EG av den 22 maj 2001 om harmonisering av vissa aspekter av upphovsrätt och närstående rättigheter inom det immaterialrättsliga området.

Europaparlamentets och rådets direktiv 2000/31/EG av den 8 juni 2000 om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden.

Europaparlamentets och rådets direktiv 2011/83/EU av den 25 oktober 2011 om konsumenträttigheter och om ändring av rådets direktiv 93/13/EEG och Europaparlamentets och rådets direktiv 1999/44/EG och om upphävande av rådets direktiv 85/577/EEG och Europaparlamentets och rådets direktiv 97/7/EG.

Gentschein, Anna (1997). Internet links B Legal implications. Institutet för rättsinformatik, IRI-rapport 4. Stockholm: Stockholms universitet.

Haarmann, Pirkko-Liisa (2005). Tekijänoikeus & lähioikeudet. Helsinki: Kauppakaari Oyj.

Harenko, Kristiina, Valtteri Niiranen & Pekka Tarkela (2006). Tekijänoikeus. Kommentaari ja käsikirja. Porvoo: WSOY.

Herler, Brita Kristina (2001). Upphovsrättsligt skydd av digitala musikaliska verk vid marknadsföring i Internet. Vasa: Acta Wasensia.

Herler, Brita Kristina & Alfred Streng (2010). ICT-rätten. Vasa.

Herler, Brita Kristina (2011). Upphovsrätt - särskilt vid universitet och högskolor. 5 rev.uppl. Vasa.

Herler, Brita Kristina & Alfred Streng (2013). Kommentarer till konsumentskyddslagen. Del I och II. 5 rev.uppl. Vasa.

Komiteanmietintö-Kommittébetänkande 1953:5. Ehdotus laiksi tekijänoikeudesta kirjallisiin ja taiteellisiin teoksiin. Helsinki: Opetusministeriö.

Komiteanmietintö-Kommittébetänkande 2002: 5. Upphovsrätten i informationssamhället. Betänkande av upphovsrättskommissionen. Helsingfors.

Komiteanmietintö-Kommittébetänkande 2012:2. Upphovsrättskommissionens betänkande B Lösningar till digitala tidens utmaningar i Undervisnings- och kulturministeriets arbetsgrupps-promemorior och utredningar.

Lehtonen, Asko (2005). Sorvari Katariina: Vastuu tekijänoikeuden loukkauksesta. Erityisesti tietoverkkoympäristössä. Virallisen vastaväittäjän lausunto Turun yliopiston oikeustieteelliselle tiedekunnalle 26.9.2005. LM 2005, s. 986-995.

Levin, Marianne (2011). Lärobok i immaterialrätt-upphovsrätt - patenträtt - mönsterrätt - känneteckensrätt - I Sverige, EU och internationellt. Tionde upplagan. Stockholm: Norstedts Juridik AB.

Olsson, Henry (2006). Copyright. Svensk och internationell upphovsrätt. Sjunde upplagan. Stockholm: Norstedts Juridik Ab.

Pihlajarinne, Taina (2011). Lupa linkittää - Toisen aineiston hyödyntämisen tekijänoikeudelliset rajat. Helsinki: Lakimiesliiton Kustannus.

Rahnasto, Ilkka (1998). Internetoikeuden perusteet. Helsinki: Kauppakaari Oyj.

Regeringens proposition till riksdagen med förslag till lag om tillhandahållande av informations-samhällets tjänster och till lagar som har samband med dem. (2001 rd - RP 194). Helsingfors.

Regeringens proposition till riksdagen med förslag till lag om ändring av upphovsrättslagen. (2002 rd - RP 177). Helsingfors.

Regeringens proposition till riksdagen med förslag till lag om ändring av upphovsrättslagen. (2004 rd - RP 28). Helsingfors.

Regeringens proposition till Riksdagen med förslag till lag om ändring av 2 kap. i konsument-skyddslagen och av vissa lagar som har samband med den (2008 rd - RP 32). Helsingfors.

Regeringens proposition till riksdagen med förslag till lagar om ändring och temporär ändring av lagen om televisions- och radioverksamhet och om ändring av 25 b och 48 § i upphovsrättslagen. (2009 rd - RP 87). Helsingfors.

Rosén, Jan (2000a). Server Copyright Liability in Europe. Notes on the Swedish Act on Liability for Intermediaries and Two Recent Decisions of the Swedish Supreme Court. International Intellectual Property Law & Policy, Fordham University, 27.–28.4.2000.

Sanger, Lisa (1996). Caching on the Internet. Tillgänglig: <http://seamless.com/eric/cache.htm>.

Statens offentliga utredningar. SOU 1956:25. Upphovsmannarätt till litterära och konstnärliga verk. Lagförslag av auktorrättskommittén. Stockholm: Justitiedepartementet.

Still, Viveca (2007). DRM och upphovsrättens obalans. Helsingfors. IPR University Center.

Sorvari, Katariina (2005). Vastuu tekijänoikeuden loukkauksesta. Erityisesti tietoverkkoympäristössä. Helsinki: WSOY.

Sorvari, Katariina (2007). Tekijänoikeuden loukkaus. Helsinki: WSOYpro.

Streng, Alfred (2007). Ideella rättigheter i digital miljö. Vasa: Acta Wasaensia.

Tikka, Kari & Olli Nykänen (2000). Sarjatoiminta. I: Yritysverotus II: 25, 14-15. Helsinki: WSOY.

RESOLVING THE CRISIS OF COPYRIGHT LAW IN THE DIGITAL ENVIRONMENT: REFORMING THE “COPY-RIGHT” INTO A “REUSE- RIGHT”

¹Primavera De Filippi, ²Katarzyna Gracz

¹Researcher at CERSA / CNRS / Université Paris II, research fellow at the Berkman Center for Internet & Society at Harvard Law School.

pdefilippi@gmail.com

²PhD researcher at the European University Institute, Florence Law Department.

katarzyna.gracz@eui.eu

Keywords: *Copyright law, autopoiesis, digital technologies*

Abstract: *The paper explores the mechanisms that led to the current crisis of copyright law in the digital era by applying the concept of law as an autopoietic system. It analyses how copyright law has evolved over the years, and how - every time a new technology has come to disrupt the system - the law has evolved to try and preserve the traditional status quo. Today, however, in order to benefit from the new opportunities offered by digital technologies, copyright law must be radically reformed to encourage - rather than discourage - the dissemination of online works. This might require a shift from a system based on the concept of reproduction (copy-right) to a system based on the reutilization of works (reuse-right).*

1. Theoretical stance

The paper explores the mechanisms that led to the current crisis of copyright law in the digital era by applying the concept of law as an autopoietic system - as developed by Niklas Luhmann and Gunther Teubner (Luhmann, 2008; Teubner, 1988) - whereby the legal system is regarded as an autonomous, self-referential normative system that remains separate from other normative systems (such as religion, morality, or social norms), independently setting its own boundaries through a binary process that distinguishes what is *legal* from what is *illegal*.

This paper draws from systems theory to analyse the eco-system of copyright law and to describe its historical development throughout the years. The study reconstructs the mutual interplay between the **legal system** and the following elements: **technology**, **social norms** and **collective interests** of four groups representing most important actors in the copyright regime (authors, intermediaries, state authorities, and the public).

Yet, systems theory is not regarded as an ontological claim about the nature of law, but rather as a means to explain the historical pattern that characterizes the evolution of copyright law: what are the drivers of its evolution and what is the cause of its failure in the digital era. From a historical

perspective, the paper focuses on four fundamental phases that are perceived as landmarks in the development of copyright law: 1) shift from the manuscript era to the age of print, 2) advent of modern copyright law, 3) introduction of technologies allowing for mass consumer copying, 4) era of digital technologies and Internet.

In this context, the concept of self-referential social systems is used as a useful metaphor for modelling the dependencies that gave rise to the shortcomings of copyright law in the digital era and to explain the growing discrepancy that is emerging between **social** and **legal** norms. Yet, the authors do not consider this discrepancy to be inevitable, as it does not stem from the very nature of law. Quite to the opposite, it is argued that compliance with copyright law in the digital world can only be achieved once the divergence between these two normative bodies will be overcome.

2. The problem: a mismatch between legal and social norms

The paper contends that the current divergence between social and legal norms is at the source of the crisis of copyright law in the digital era - a crisis illustrating the failure of copyright law as an autopoietic system. Yet, the process of autopoiesis in copyright law did not start with the introduction of Internet and digital technologies, but actually has its roots at the inception of the copyright regime, when the proprietary paradigm was first transposed from property law into the realm of copyright law. It is argued, however, that it was not the transposition of the proprietary paradigm into the realm of intellectual creations that actually led to the current crisis of the copyright system, but rather its evolution, throughout the years, into something that is ever more akin to an absolute monopoly right.

Travelling through a variety of historical phases, the copyright system has managed to keep a proper balance between protecting the interests of right holders on one hand, and those of the general public on the other hand. For a long time, even though powerful campaigns in favour of a strong proprietary rhetoric arose with every significant technological change, the legislator did not submit to the lobbying of the cultural industry advocating for an *absolute-property* paradigm. Yet, with the advent of Internet and digital technologies - which effectively eliminated scarcity - copyright law's selective response to environmental *stimuli* resulted in its failure to adapt to the digital reality. The delicate equilibrium of the copyright regime has progressively been disrupted through a series of legislative reforms aimed at adjusting the law to the digital environment, mainly focusing on furthering the commercial interests of the cultural industry, at the expense of the public and in certain cases of the authors (as illustrated by the recent debates around ACTA). This eventually led to the degeneration of the proprietary paradigm (which had been formerly transposed from the realm of property law into the realm of intellectual property law), by turning a limited monopoly right over information into a right which has become gradually more encompassing than its physical counterpart.

The authors claim that by stubbornly trying to apply old and inadequate patterns to an entirely new context, the law did not adapt satisfactorily to the digital world. Rather than understanding and taking advantages of the new opportunities offered by digital technologies, the law attempted to replicate the rules of the physical world into the digital world by providing extensive protection to the interests of right holders, often at the expense of the public's general interest.

This, along with the progressive removal of the creative author from the value chain (increasingly controlled by large corporations or collecting societies), the belligerent strategies of copyright holders in the fight against copyright infringement, the increasing number of criminal prosecution against end-users, as well as the linguistic battles describing individuals as "pirates" even when they operate

outside of the commercial sphere, is what - according to the authors - has mostly contributed to today's negative perception of copyright law by the general public.

The paper contends the law has distanced itself so much from social norms and the technological context in which it operates, that it has nowadays lost most of its credibility and applicability in the digital era. As a result of this divergence between legal norms (restricting the use and reuse of information) and social norms (advocating for the free circulation of knowledge on the Internet), many activities which are actually disrespectful of the law (such as the practices of file-sharing, remix or mash-ups) are not perceived negatively by end-users even though they constitute copyright infringement.

3. The solution: from “*copy-right*” to “*reuse-right*”

Digital technologies and the social norms of sharing that have progressively emerged on the Internet promoted a shift from a situation of *information scarcity* to a situation of *information overload*: users need no longer struggle to find good online content; the main struggle consists, on the contrary, in finding a public for such content.

This shift radically changed the rules of the game in terms of content production and consumption: from a situation where content is being *pushed* to the consumer to a situation where content is being *pulled* by the consumer. Internet users thus assume an important new role in assessing the quality of the content they consume: their preferences determine the type of content that will most likely be produced and the modalities under which it should be made available to the public. In particular, in a situation of information overflow - where the consumption of information constitutes an indicator of its extrinsic quality - dissemination can enhance the value of information (as perceived by the public) by creating more opportunities for consumption. Thus, the growing availability of free content online requires a careful reconsideration of the copyright regime with a view of understanding whether, and how, copyright law could eventually adapt to the digital world by better taking into account - and benefiting from - the new opportunities provided by Internet and ICT technologies.

The authors believe that, if the goal is to restore the traditional balance of copyright law in the digital environment, the copyright regime must evolve into a less restrictive system of property rights. Yet, if one considers the legislative reforms undertaken thus far, it appears that the copyright has actually evolved towards a greater degree of exclusivity. Thus, it is argued that the legal system did not properly '*understand*' or simply '*refused*' to adjust to the specificities of digital technologies. Hence, the authors contend that, in order for the copyright regime to better comply with the new environment in which it operates, it must be radically reformed.

To begin with, it should be understood that the exclusive right of reproduction has progressively gone obsolete on the Internet. In the digital environment, where every use of a work necessarily entails a reproduction thereof, reproduction can no longer be regarded as a good indicator for infringement. On the contrary, endowing right holders with the ability to restrain the reproduction of a work implies granting them control not only over the reproduction, but also over the mere consumption of that work - thereby turning *copyright* into some kind of *access right*.

Besides, to the extent that users are increasingly reluctant to pay for a good that is neither exclusive nor rival and that is often freely available on the Internet, digital media question the legitimacy of the current copyright regime stuck on preserving the interests of a deprecated industry. The law needs to acknowledge that the 'cultural industries' (as we know them today) will have a hard time surviving on the Internet. Faced with an increasing amount of content (be it commercial content or user-generated-

content) freely accessible online (both legally and illegally), the cultural industries will eventually have to evolve and experiment with new business models which are not directly related to the reproduction right.

Finally, the shift from a situation of *information scarcity* to a situation of *information overflow* welcomes the intervention of new intermediaries that feature a completely different relationship to content. On the one hand, **device producers** are a specific type of intermediaries that merely use content (such as music, movies, e-books, etc) as a means to sell something else (such as music players, e-books readers, and so forth). While such content is absolutely necessary to provide value to the consumer, it does not actually generate value *per se*: its distribution is merely instrumental to the sale of devices. On the other hand, we observe the emergence of new intermediaries whose purpose is not to provide content, but to arrange a public for that content. Those are the so-called **infomediaries** which assume the important function of gathering, organizing, and linking content and information available on the web.

To conclude, the authors contend that all actors involved in the copyright value chain - be them authors, intermediaries, or end-users - share the common objective of maximizing the value and visibility of digital works. As such, they would all benefit from a reform of copyright law that would actually encourage (rather than constrain) the reproduction and dissemination of creative works. Indeed, if consumption is an indicator of the quality of online content, the broader such content is disseminated, the more it will be able to “acquire” value. Copyright law should therefore be aimed at encouraging - rather than discouraging - the reproduction and dissemination of online works. This could be done, for instance, by reforming the law so as to no longer focus on the reproduction and distribution rights, but only and exclusively on reuse rights.

4. References

- Bain Read, ‘Technology and State Government’, *American Sociological Review*, Vol. 2 (6) (1937),
- Brian Skyrms (eds), *The Dynamics Of Norms*, (New York: Cambridge University Press, 1997)
- Carr David McLain, *Writing on the Tablet of the Heart: Origins of Scripture and Literature*, (Oxford University Press 2005);
- Christina Bicchieri, *Learning To Cooperate*, in Christina Bicchieri, Richard Jeffry
- Dennis Wrong, *The Problem Of Order: What Unites and Divides a Society* (New York: Free Press, 1994)
- Diane E.Booton, *The Librarius and Libraire as Witnesses to the Evolving Book Trade in Ducal Brittany in Pécia*, (2010),
- Emile Durkheim, *The Determination of Moral Facts*, in *Sociology and Philosophy* (London: Cohen and West, [1903] 1953)
- Jane Ginsburg, ‘A Tale of Two Copyrights: Literary Property in Revolutionary France and America’, 64 *Tulane Law Review*, 64(5), May 1990
- Hector L.MacQueen, Charlotte Waelde and Laurie T.Graeme, *Contemporary Intellectual Property: Law and Policy* (Oxford University Press, 2007),
- Homans George C., *Social Behavior: Its Elementary Forms* (New York: Harcourt, Brace 1961)
- Hughes, J. (1988). *The Philosophy of Intellectual Property*. *Georgetown Law Journal* 7777(287).
- Mark Rose, ‘Copyright and its Metaphors’ (2002) 50 *UCLA Law Review*, 1

Mark Rose, *Authors and Owners: The Invention of Copyright* (Cambridge, Mass: Harvard University Press, 1993).

O'Brien, D. S., & Fitzgerald, B. F. 'Mashups, remixes and copyright law'. (2006) *Internet Law Bulletin*, 9(2).

Peter Damerow, *Abstraction and Representation: Essays on the Cultural Evolution of Thinking*, (Springer, 1996);

Rowan Watson, *Illuminated Manuscripts and Their Makers* (Victoria & Albert Museum, 2003),

Talcott Parsons, *The Social System* (New York: Free Press, 1952)

Tylert T. Ochoa, *Copyright Duration: Theories and Practice* in: Peter Yu, *Intellectual Property and Information Wealth: Issues and Practices in the Digital Age* (Westport Conn.: Praeger Publishers, 2007).

ON SCRIPTURA, PRINTING AND THE ORIGINS OF COPYRIGHT

Mariagrazia Rizzi¹, Georg Jakob²

¹Ricercatore confermato e professore aggregato presso il Dipartimento dei Sistemi Giuridici, Università degli Studi di Milano-Bicocca

mariagrazia.rizzi@unimib.it

²Mag. iur., Founder and Managing Director of patalyst.com - Patent research & visualization

gj@patalyst.com

Keywords: *Accessio, Gai. 2.77-78, Gai 2 Rer. cott. D. 41.1.9.1, Printing Press, Statute of Anne, Bookseller's Guild, Labour Theory of Property, Immanuel Kant, Johann Gottlieb Fichte, Reprinting of Books, Author's Rights*

Abstract: *Today, the origin of copyright and author's rights is almost always seen as closely tied to Johannes Gutenberg's invention of mechanical printing in the first half of the 15th century while the Statute of Anne, enacted in 1710 is usually cited as the first "Copyright Act" in a modern sense. But there is also a school of thought suggesting tracing the roots of legal protection of authorship as far back as ancient Rome. This paper takes a critical look at both of these approaches. It is argued that the problem of copyright and author's rights was never mainly about to whom such a right is supposed to be assigned, but much more and in the first place in what such a right actually consists. It is, in other words, not about a property right in the classical, let alone material sense, but about where exactly the lines are to be drawn that define said right. We conclude that this problem was not solved before Immanuel Kant and Johann Gottlieb Fichte, when mechanical printing already had become a widespread technology and book-selling a viable industry across Europe and that the philosophical and political thought of the Age of Enlightenment was essential in the creation of copyright and author's rights.*

1. Die Frage nach den Ursprüngen des Urheberrechts wie wir es heute kennen, ist ein Gebiet auf dem zwar in groben Zügen Übereinstimmung zu herrschen scheint, auf dem sich aber auch missverständliche und zum Teil widersprüchliche Meinungen gegenüberstehen. Nach der wohl am weitesten verbreiteten Auffassung ist die moderne Urheberrechtsordnung auf die Einführung des Buchdrucks zurückzuführen¹. Der Tatsache, dass zwischen der Erfindung des Buchdrucks und dem ersten nachweisbaren Auftreten des Begriffs Urheberrecht in einem Gesetzesentwurf mehr als vier Jahrhunderte liegen², findet dabei nicht immer ausreichende Beachtung³.

¹ Vgl. beispielsweise etwa M. Rehbinder, Urheberrecht, 16. Aufl., München 2010, S. 7 ff.; U. Izzo, Alle origini del copyright e del diritto d'autore, Rom 2010, S. 45 ff.; A. D'Aamato/D.E. Long, International Intellectual Property Law, London 1997, S. 76; alle m.w.N.

² Und zwar in einem Entwurf des Börsenvereins Deutschen Buchhandels von 1857, vgl. C. Reinhardt, Die Grundlagen Des Urheber- und Verlagsrechts in Deutschland im 17. und frühen 18. Jahrhundert, Norderstedt 2010, S. 15.

Andererseits wollen einige Autoren die Wurzeln des Urheberrechts viel früher und zwar schon in der römischen Antike, sehen⁴. Zum Teil werden hier schon die Anfänge eines Urheberpersönlichkeitsrechts bejaht⁵, andere Autoren postulieren einen Rechtsschutz ökonomischer Interessen der Urheber⁶. Insbesondere Ugo Bartocci hat in jüngerer Zeit versucht, „un primo embrionale orientamento nella direzione che porterà, attraverso una secolare elaborazione dottrinale e passando per la concettualizzazione, elaborata nell'età moderna, della proprietà letteraria, alla definizione di quello che verrà poi comunemente indicato in forma sintetica come diritto di autore“⁷ zu identifizieren.

Wenn wir davon ausgehen, dass mindestens zwei Elemente nötig sind, um von einem Urheberrecht im heutigen Sinne sprechen zu können⁸, nämlich erstens die grundlegende Abstraktion des unkörperlichen Werks, der geistigen Schöpfung (z.B. ein Gedicht oder Roman) von seinem materiellem Träger (das Papier, auf dem es gedruckt wird) sowie zweitens, die rechtliche Anerkennung einer Verbindung dieses Werkes mit seinem Schöpfer, dem Urheber, dann verdienen diese Überlegungen eine durchaus kritische Betrachtung.

2. Die Theorie von Bartocci⁹ basiert auf einer neuen Lesart eines der wichtigsten juristischen Zeugnisse zum Thema *scriptura*, und zwar Gai. 2.77:

Gai 2.77: *Eadem ratione probatum est, quod in chartulis sive membranis meis aliquis scripserit, licet aureis litteris, meum esse, quia litterae chartulis sive membranis cedunt.*

Bartocci vertritt die Auffassung, Gaius würde im vorliegenden Text den Fall untersuchen, dass jemand, der Eigentümer der zu beschreibenden Unterlage und gleichzeitig Autor des darauf zu schreibenden Werkes sei, letzteres einem *scriba* diktieren würde. Aufgrund dieses Textverständnisses meint Bartocci nun, der Grundsatz, die Buchstaben würden dem Papier folgen, sei die Antwort „ad un'esigenza concreta: la necessità cioè di poter attribuire la proprietà di un testo a persona diversa dallo scrivente qualora questi non ne fosse l'autore“¹⁰. Da der Schutz eines Verfassers von einem Schriftwerk als *res incorporalis*¹¹ in Rom undenkbar gewesen sei, schließt er, „il rimedio che il sistema giuridico romano trovò per proteggere l'autore, non poté che essere inquadrato in uno dei mezzi di acquisto della proprietà già previsti per le *res corporales*“¹². Weil beim Verfassen von Literaturwerken so häufig auf

³ Andererseits widmete in jüngerer Zeit E. Höffner mit dem zweibändigen Opus Geschichte und Wesen des Urheberrechts, Band I und II, München, 2010/11, diesem Zeitraum eine detailreiche und über weite Strecken bahnbrechende Untersuchung, auf die im folgenden noch mehrfach zu verweisen sein wird.

⁴ Für eine Darstellung der dazu geäußerten Hypothesen vgl. U. Bartocci, Aspetti giuridici dell'attività letteraria in Roma Antica. Il complesso percorso verso il riconoscimento dei diritti degli autori, Torino 2009, 93 ff. m.w.N.

⁵ Siehe dazu die Nachweise bei U. Bartocci, Aspetti giuridici dell'attività letteraria cit., S. 98 ff. und S. 117 ff.

⁶ Dazu nochmals U. Bartocci, Aspetti giuridici dell'attività letteraria cit., S. 110 ff.

⁷ U. Bartocci, Aspetti giuridici dell'attività letteraria cit., S. 233.

⁸ Ausführlich M. Rehinder, Urheberrecht cit., S. 23 ff.

⁹ Vgl. dazu die Rezensionen von G. Santucci, *Diritti dell'autore in Roma antica?*, in *Index* 39 (2011), S. 143 ff.; P. Cerami, *Recensione di U. Bartocci, Aspetti giuridici dell'attività letteraria in Roma antica. Il complesso percorso verso il riconoscimento dei diritti degli autori*, in *IVRA* 59 (2011), S. 291 ff.

¹⁰ U. Bartocci, *Aspetti giuridici dell'attività letteraria* cit., S. 20.

¹¹ Wie Bartocci selbst unter Bezugnahme auf und Vertiefung von Überlegungen, die in der Literatur bereits mehrfach angestellt wurden, ausführlich darlegt (U. Bartocci, *Aspetti giuridici dell'attività letteraria* cit., S. 106 ff.), wurde im Römische Recht nie eine Eigentum an unkörperlichen Sachen entwickelt, da das Eigentumsrecht vollständig auf eine *res* bezogen war und andererseits dieses Recht auf keine Art in das Konzept der *res incorporales* zu integrieren war. Zum Problem der Abgrenzung von *res incorporales* im Römischen und im zeitgenössischen Recht vgl. zuletzt G. Turelli, *Res incorporales e beni immateriali: categorie affini, ma non congruenti*, in <http://www.teoriaestoriadeldirittoprivato.com/index.php?com=statics&option=index&cID=258>.

¹² U. Bartocci, *Aspetti giuridici dell'attività letteraria* cit., S. 129 Fn. 129.

scribae zurückgegriffen worden sei, wäre dieser Schutz über die Regeln zur *accessio* verwirklicht worden.

Um seine These zu stützen, untersucht Bartocci in der Folge die zum gaianischen Text korrespondierende Stelle aus den *Res cottidianae*:

Gai 2 *Rer. cott.* D. 41.1.9.1: *Litterae quoque licet aureae sint perinde chartis membranisque cedunt, ac solo cedere solent ea quae aedificantur aut seruntur. Ideoque si in chartis membranisque tuis carmen vel historiam vel orationem scripsero, huius corporis non ego, sed tu dominus esse intellegeris.*

Er zeigt auf, worin sich der in den Institutionen untersuchte Fall von jenem in den *Res cottidianae* unterscheidet: im Gegensatz zu ersterem ging es in letzterem nämlich um ein Werk, das der Autor selbst auf der Unterlage eines anderen verfasst habe. Demnach wären die Rollen in den *Res cottidianae* gegenüber dem gaianischen Passus gewissermaßen invertiert, der Schreiber ist hier auch der Werkautor, während das Papier einem Dritten gehört. Ausgehend von dieser Erkenntnis, die er für keineswegs zufällig hält, kommt er dann zu einem weiteren Unterschied zwischen den Texten, der Bezugnahme auf das Schreiben eines *carmen*, einer *historia* oder einer *oratio*. Nach ihm wären diese drei Beispiele, anders als von einem Teil der Lehre angenommen eben keine „aggiunta superflua“, sondern vielmehr in Richtung einer Akzentuierung des Schöpfers eines literarischen Werkes zu lesen.

3. Obgleich diese These zugegebenermaßen verlockend ist, erscheinen die zu ihrer Untermauerung vorgebrachten Elemente, wie zum Teil auch schon in der Literatur dargelegt wurde, doch zu schwach um sie als gesichert anzunehmen¹³. Abgesehen davon, dass keineswegs klar ist, in welchem Ausmaß die Arbeit nicht versklavter *scribae* zur Niederschrift von Texten in Anspruch genommen wurde¹⁴, und dass darüber hinaus auch der von Bartocci behauptete überwiegende Einsatz von Diktaten beim Verfassen von Texten nicht feststeht¹⁵, lässt sich eben nicht mit Sicherheit nachweisen, Gaius hätte in seiner Darstellung der Verbindung von Schrift und Papier in den Institutionen gerade den speziellen

¹³ Die Arbeit Bartoccis wurde kritisch untersucht von G. Santucci, *Diritto romano e diritti europei. Continuità e discontinuità nelle figure giuridiche*, Bologna 2010, S. 35 f.; Id., *Diritti dell'autore in Roma antica?*, in *Index* 39 (2011), S. 143 ff.

¹⁴ Dieser Einwand wurde bereits vertieft von G. Santucci, *Diritto romano e diritti europei* cit., S. 35 Fn. 79; Id., *Diritti dell'autore* cit., 145 f.

Weniger entscheidend dagegen die auf Paul. 21 *ad ed.* D. 6.1.23.3 (*Sed et id, quod in charta mea scribitur aut in tabula pingitur, statim meum fit: licet de pictura quidam contra senserint propter pretium picturae: sed necesse est ei rei cedi, quod sine illa esse non potest*) gestützte Anmerkung von Santucci. Er meint nämlich (*Diritto romano e diritti europei* cit., S. 36 und Fn. 82; Id., *Diritti d'autore* cit., S. 144 und Fn. 4) bezüglich dieser Stelle „si giustifica l'acquisto della *scriptura* al proprietario della *charta* per il semplice ed incontestabile principio logico che la scrittura presuppone necessariamente il supporto materiale e, non potendo venire ad esistenza senza di esso, ad esso deve essere subordinato“. Dem ist allerdings entgegenzuhalten, dass die Erklärung von Paulus, obwohl explizit nur von Malerei die Rede ist, auch auf die Literatur anwendbar ist, hinsichtlich der Malerei eben nicht von allen Juristen geteilt wurde, da ein Teil von ihnen, wie im Übrigen nicht nur aus der Paulus-Stelle selbst, sondern darüber hinaus aus den Institutionen des Gaius, den *Res cottidianae* sowie den Institutionen des Iustinian hervorgeht, der Ansicht war, der Maler sollte, offenbar auf der Basis einer anderen Begründung, obsiegen. Mit anderen Worten war für einen Teil der Juristen der Umstand, dass eine Malerei nicht ohne materiellen Träger existieren kann, kein akzeptables Argument das dazu ausreichend oder dafür entscheidend sein konnte, den Eigentümer der Tafel obsiegen zu lassen. Folglich lässt sich nicht generell ausschließen, dass auch die *scriptura* betreffend einige Juristen von einer entsprechenden Begründung nicht überzeugt gewesen sein mochten.

¹⁵ Auch diese Kritik wurde bereits von G. Santucci, *Diritto romano e diritti europei* cit., S. 35 Fn. 79; Id., *Diritti dell'autore* cit., S. 144, entwickelt, der betont wie „dalla maggior parte delle testimonianze letterarie prodotte a sostegno di questa interpretazione, si può argomentare *e contrariis*, in quanto in non pochi casi si tratta di situazioni in cui gli autori ricorrono alla dettatura in ragione di un impedimento fisico o materiale“. Zurückkommend auf die auch von Bartocci ausführlich untersuchte Ulp. 24 *ad ed.* D. 10.4.3.14 (vgl. *infra* Fn. 14) legt er dann dar, dass es um eine „vicenda affatto peculiare che certamente non può essere assunta come modello di una prassi“ gehe (145).

Fall der Niederschrift eines Werkes durch einen *scribae* auf Papier, das dem eigentlichen Autor des Werks gehört, im Auge. Zunächst einmal führt er den Diskurs über die *scriptura* im Rahmen einer ausführlicheren Behandlung der *accessio*¹⁶ und im Besonderen des Grundsatzes *superficies solo cedit*, welcher sozusagen den „roten Faden“ seiner Betrachtungen darstellt. Er erwähnt diesen Grundsatz im Paragraph 73, wo er den Fall des Bauens auf fremdem Grund und Boden beschreibt. Auf ihn bezieht er sich auch in den folgenden zwei Beispielen, der *implantatio* respektive der *satio*: in beiden Fällen soll es der *dominus* des Grundstücks sein, der Eigentum an den Pflanzen bzw. den Saatgut erwirbt¹⁷. Diesen Fällen stellt Gaius nun den des Schreibens zur Seite, wobei er das Papier dem Boden gleichstellt und auf diese Weise schlüssig zum Obsiegen des Eigentümers über den Schreibenden kommt¹⁸.

Andererseits ist der gesamte Abschnitt über die *accessio* so abgefasst, dass der Eigentümer derjenigen Sache, welcher die jeweils andere zufällt, in der ersten Person Singular¹⁹ bezeichnet ist, der jeweils andere dagegen in der dritten Person Singular. In Gai 2.73 ist „ich“ also der Grundeigentümer auf dessen Grundstück gebaut wird, in 2.74 der, auf dessen Grund gepflanzt wird und in 2.75 der *dominus* auf dessen Grund gesät wird. Auf diese Beispiele folgt direkt jenes des Schreibens, es scheint mithin also völlig selbstverständlich, dass hier im Einklang mit den zuvor erwähnten Beispielen, Gaius, der ja die Unterlage, Papyrus oder Pergament, hier analog zum Grundstück behandelt, den Eigentümer ersterer wiederum in der ersten Person und denjenigen, der die Schrift darauf aufbringt, in der dritten Person bezeichnet. Im darauf folgendem Beispiel der *pictura* finden wir wiederum den Maler in der dritten und den Eigentümer der *tabula* in der ersten Person Singular:

Gai. 2.78: *sed si in tabula mea aliquis pinxerit veluti imaginem, contra probatur; magis enim dicitur tabulam picturae cedere.*

Die Bezeichnung des *dominus tabulae* in der ersten Person Singular und die Formulierung *is qui pinxerit* in der dritten Person²⁰ führt also die anfangs eingeschlagene Aufteilung einmal mehr konsequent weiter. Dass aber der Maler auch der Schöpfer des Gemäldes ist, steht zweifelsfrei fest und obwohl in diesem Beispiel, im Gegensatz zu dem beim Beispiel des Schreibens festgestelltem, der Eigentümer des Untergrundes unterliegt, denkt Gaius offenbar nicht daran, den bisher durchgehaltenen grammatikalischen Aufbau abzuändern²¹.

¹⁶ Zu dieser vgl. unter den jüngeren Beiträgen, P. Pasquino, *Rimedi pretori in alcuni casi di accessione*, in *Teoria e Storia del Diritto Privato* 4 (2011), *passim*.

¹⁷ Gai. 2.73: *Praeterea id quod in solo nostro ab aliquo aedificatum est, quamvis ille suo nomine aedificaverit, iure naturali nostrum fit, quia superficies solo cedit.* 74. *Multoque magis id accidit et in planta, quam quis in solo nostro posuerit, si modo radicibus terram complexa fuerit.* 75. *Idem contingit et in frumento, quod in solo nostro ab aliquo satum fuerit.* 76. *Sed si ab eo petamus fundum vel aedificium et impensas in aedificium vel in seminaria vel in sementem factas ei solvere nolimus, poterit nos per exceptionem doli mali repellere, utique si bonae fidei possessor fuerit.*

¹⁸ Vgl. auch G. Santucci, *Diritto romano e diritti europei* cit., S. 35 f.

¹⁹ Dieser Aspekt wird auch von A. Plisecka, *Tabula picta. Aspetti giuridici del lavoro pittorico in Roma antica*, Padova 2011, S. 90, erwähnt, die dazu erklärt „tale plastico e conseguente linguaggio corrisponde al carattere didattico dell’opera“.

²⁰ Während im folgenden Teil das „ich“ unverändert auf den Eigentümer des beschriebenen Untergrunds bezogen bleibt, wird der Schreibende nun in der zweiten Person bezeichnet (...*certe secundum hanc regulam si me possidente petas imaginem tuam esse, nec solvas pretium tabulae, poteris per exceptionem doli mali summovei; at si tu possideas, consequens est, ut utilis mihi actio adversum te dari debeat: quo casu nisi solvam impensam picturae, poteris me per exceptionem doli mali repellere, utique si bonae fidei possessor fueris. illud palam est, quod sive tu subriperis tabulam sive alius, competit mihi furti actio*), was für unsere Überlegungen jedoch unbeachtlich bleibt.

²¹ Hinsichtlich des Verhältnisses von *scriptura* und *pictura* scheinen sich, wie zutreffend festgestellt wurde, noch weitere Überlegungen zu ergeben. Auf der Grundlage seiner oben besprochenen Interpretation von Gai. 2.77 meint Bartocci,

4. Darüber noch hinausgehende Überlegungen ergeben sich im Hinblick auf den korrespondierenden, der *scriptura* gewidmeten Passus der *Res cottidianae* sowie dessen Verhältnis zum oben besprochenen Text der Institutionen des Gaius. Betreffend die Stelle D. 41.1.9.1 meint Bartocci ja, sie unterscheide sich von Gai. 2.78. Dazu kommt er offensichtlich angesichts der Tatsache, dass es sich in der Stelle aus den *Res cottidianae* bei dem in der ersten Person benannten Subjekt um den Schreibenden handelt. Dies bringt ihn dann zu der Beobachtung, dass es hier um den Schöpfer eines literarischen Werks geht, der den Untergrund eines anderen beschrieben habe.

Obzwar es zutrifft, dass in den *Res cottidianae* für bestimmte Probleme Lösungen zu finden sind, die sich von jenen der *institutiones* unterscheiden²², so scheinen für den hier in Frage stehenden Fall keine ausreichenden Indizien vorzuliegen, die eine Hypothese wie die von Bartocci vorgeschlagene nahelegen würden. Was die Unterscheidung der literarischen Genres *carmen*, *historia* und *oratio* betrifft, auf die wie oben schon angedeutet Bartocci abstellt, lässt sich unter Bezugnahme auf die bisherigen Analysen argumentieren, es ginge hier um den Umfang des Geschriebenen und damit um die Menge an verwendeter und daher mit dem Papyrus oder Pergament verbundener Tinte. Hinsichtlich des Subjektwechsels, der nach Bartocci ein weiteres Element sein soll, der die Aufmerksamkeit des Juristen auf den Autor des Schriftwerks unterstreichen soll, bietet sich ein Vergleich des Textes der *Res cottidianae* mit jenem der Institutionen des Justinian²³ sowie mit der Paraphrase des Theophilus an. In den Institutionen Justinians wird die *accessio* des Geschriebenen an die Unterlage mit einem den Eigentümer bezeichnenden „Du“ in der zweiten und der schreibende *Titius* in der dritten Person beschrieben. Wie in den *Res cottidianae* ist also der schreibende auch Autor des Werks, nur dass hier von ihm in der dritten und nicht in der ersten Person die Rede ist. Bei Theophilus wird der Fall nun in folgender Weise geschildert: der Eigentümer der Unterlage wird mit „Ego“ bezeichnet, der schreibende wiederum in der dritten Person Singular. Wenn es nun tatsächlich darum gegangen wäre, die Autorenschaft am Werk zu betonen, so sollte derselbe Aufbau von Subjekt und Objekt, respektive Eigentümer der Unterlage und der auf dieser schreibende auch in den Institutionen des Justinian und der Paraphrase des Theophilus zu finden sein.

Will man also nicht ein ganz spezielles Augenmerk des Gaius auf die Schöpfer literarischer Werke²⁵ annehmen, eine Sensibilität die dann in der folgenden Epoche vergessen worden sein müsste, ergibt sich ein weiteres Argument dafür, dass den hier besprochenen Stellen der Gedanken an eine rechtliche Beachtlichkeit der Autorenschaft von Schriftwerken schlicht und einfach fremd ist. Abgesehen von der Unwahrscheinlichkeit eines Perspektivenwechsels wie er hier besprochen wurde, gibt es einen weiteren

sowohl im Fall der *scriptura* als auch in jenem der *pictura* sei es die Intention des Juristen gewesen, den Autor zu schützen. Insoweit es tatsächlich zutrifft, dass die von Gaius dargestellte, den Maler über den Eigentümer der Tafel obsiegen lassende Lösung dem widerspricht, was man nach dem Grundsatz *superficies solo cedit* erwarten dürfte, so bliebe dennoch nachzuweisen, dass diese Lösung tatsächlich den Maler als Urheber des Gemäldes schützen will, dazu zuletzt M. Rizzi, G. Jakob, *Tabula Picta und Bildende Kunst: über Ursprünge und Gegenwart des Urheberrechts*, in: Zeichen und Zauber des Rechts - Festschrift für Friedrich Lachmayer zum 70. Geburtstag, Wien 2013 (im Druck).

²² Für eine Zusammenstellung und Analyse der verschiedenen Stellen der *Res cottidianae* und ihrer jeweiligen Pendants in den *institutiones* vgl. neben anderen A. Cenderelli, *Il trattato e il manuale: divagazioni in tema di "res cottidianae"*, in *BIDR* 101-102 (1998-99), S. 61 ff. (= *Scritti romanistici*, Milano 2011, S. 591 ff.).

²³ I. 2.1.33: *litterae quoque, licet aureae sint, perinde chartis membranisque cedunt, acsi solo cedere solent ea quae inaedificantur aut inseruntur: ideoque si in chartis membranisque tuis carmen vel historiam vel orationem Titius scripserit, huius corporis non Titius, sed tu dominus esse iudicaris.*

²⁵ Es soll nicht unerwähnt bleiben, dass auch Julian, Ulpian und Paulus ohne jeden Zweifel das Prinzip vertreten, dass die Schrift dem Schicksal der beschriebenen Unterlage folgt, vgl. Ulp. 24 *ad ed.* D. 10.4.3.14: *... Ait Iulianus, si quidem mea charta scriptae sint, locum esse huic actioni, quia et vindicare eas possum: nam cum charta mea sit, et quod scriptum est meum est: sed si charta mea non fuit, quia vindicare non possum, nec ad exhibendum experiri: in factum igitur mihi actionem competere*; Paul. 21 *ad ed.* D. 6.1.23.3 (Dazu oben Fn. 13).

Einwand, der die Hypothese einer besonderen Beachtung von Autoren durch Gaius²⁶ auf noch schwächeren Füßen stehen lässt. Will man dieser nämlich folgen, so verbliebe derjenige Autor, der sein Werk eigenhändig auf dem Papier eines anderen niederschreibt, gänzlich ohne Schutz. Keinesfalls lässt sich nun aber annehmen, dass dieser Fall anders als nach der in Paragraph 77 aufgestellten Regel behandelt werden soll; dazu fehlt schlicht und einfach jedweder Hinweis in den Quellen. Sollte es aber andererseits tatsächlich zutreffen, dass das eigenhändige Niederschreiben von Werken gegenüber dem Diktat nur selten vorgekommen sein sollte, so bleibt aber dennoch die Tatsache, dass in den erwähnten Texten der *Res cottidianae*, der Institutionen des Julian sowie in der Paraphrase des Theophilus ganz ohne Zweifel genau davon die Rede ist. Insgesamt erscheint es daher nur schwerlich vertretbar, in den Institutionen des Gaius eine andere Fallkonstellation annehmen zu wollen, als in allen anderen hier besprochenen Texten, die sich mit dem Verhältnis *tabula/scriptura* befassen.

5. Ganz überwiegend wird die Geburtsstunde des Urheberrechts heute mit der Erfindung des Buchdrucks mit beweglichen Lettern um 1455 durch Johannes Gutenberg in Verbindung gebracht²⁷. Zwar besteht diese Verbindung tatsächlich - schon der englische Begriff des Copyright spricht für dieses Verständnis - allerdings war es ein langer Weg bis zur tatsächlichen rechtlichen Anerkennung von Autorenrechten, der durch mehrere Jahrhunderte führte. Als legislativer Wendepunkt²⁸, gar als erstes modernes Urheberrechtsgesetz²⁹, wird üblicherweise das Statute of Anne von 1710 betrachtet. In den vorhergehenden Jahrhunderten hatte sich in Europa ein in den Details zwar unterschiedliches, in seinen grundlegenden Prinzipien folgendermaßen ablaufendes System verbreitet: die jeweiligen Landesfürsten gewährten sogenannte Druckerprivilegien, d.h. bestimmte Verleger erhielten das ausschließliche Recht bestimmte Werke für das jeweilige Territorium zu drucken und zu verkaufen. Dabei ging es nicht nur um den Schutz der wirtschaftlichen Interessen der Drucker und Buchhändler, vielmehr waren für die Feudalherren Zensurinteressen im Spiel, spätestens seit der Reformation war ihnen klar, wie gefährlich das geschriebene Wort sein konnte³⁰. In England wurde die Booksellers Guild³¹ mit hoheitlichen Befugnissen³² ausgestattet, verteilte die einzelnen Abdruckrechte monopolistisch an ihre Mitglieder und übte die Inhaltskontrolle über die zu veröffentlichenden Werke aus. Die Autoren spielten eine vergleichsweise untergeordnete Rolle. Sobald sie ihr Manuskript beim Verleger abgegeben hatten, waren es letztere, der über Auflagenzahl und -stärke, Aufmachung und etwaige Änderungen entschied und nicht zuletzt war er derjenige, der die Einnahmen aus dem Verkauf einstrich. Das Statute of Anne wird heute insofern überbewertet, als es darin nicht unbedingt und vorrangig darum ging, die Stellung der Autoren zu verbessern. Zwar war die Zustimmung des Autors zur Veröffentlichung nun auch formell nötig, das alleine änderte aber an der bisherigen Situation wenig. Zunächst ist ja der Autor im Besitz seines Manuskripts, er entscheidet also, ob er es einem Verleger ggf. gegen entsprechende Bezahlung zum Abdruck überlässt. Was das Statute of Anne nun einführte, war eine zeitliche Befristung von 14 Jahren, die sich um weitere 14 Jahre verlängerte, wenn dieser bei Ablauf der ersten Frist noch am Leben war. Danach wurde das betroffene Werk gemeinfrei.

²⁶ Dies deutet auch A. Plisecka, *Tabula picta* cit., S. 91 Fn. 106 an.

²⁷ Vgl. dazu nochmals die oben in Fn. 1 zitierten Nachweise.

²⁸ R. Kühlen, *Erfolgreiches Scheitern - eine Götterdämmerung des Urheberrechts?*, Boizenburg 2008, S. 69.

²⁹ So etwa M. Rimmer, *Digital Copyright and the Consumer Revolution*, Cheltenham 2007, S. 4; ähnlich A. D'Aamato/D.E. Long, *International Intellectual Property Law* cit., S. 76. Vgl. dazu auch L. Giesecke, *Vom Privileg zum Urheberrecht*, Göttingen 1995, S. 138.

³⁰ E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 37 ff.

³¹ Ihre Mitglieder erwarben Manuskripte, gaben deren Druck in Auftrag, und verkauften *en gros* an die eigentlichen Buchhandlungen, wären also aus heutiger Sicht eher als Verleger bzw. *publisher* zu bezeichnen, E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 60.

³² E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 58.

Wie Höffner recht überzeugend darlegen konnte, war das vorrangige Ziel nicht, den Urheber zu schützen, sondern den Wettbewerb unter den Verlegern zu regeln³³. Denn da das Ausschließlichkeitsrecht des Autors nun ein Ablaufdatum hatte, konnte er nur ein befristetes recht übertragen. Nach dessen Ablauf war plötzlich Konkurrenz unter den Verlegern möglich. Diese Interpretation scheint auch deshalb überzeugend, weil sich in England im 16. und 17. Jahrhundert ein ausgeprägtes Monopolproblem entwickelt hatte, das eine ganze Reihe von Märkten betraf, da der Handel mit zahlreichen, oft auch lebensnotwendigen Gütern über Patente und Privilegien geregelt und so mit den auch heute noch typischerweise mit Monopolen in Verbindung gebrachten Nachteilen, wie niedrige Qualität der erhältlichen Produkte bei überhöhten Preisen, verbundenen war. Das Parlament versuchte diese Monopole daher 1624 - weitgehend erfolgreich - aufzubrechen, und zwar mit dem *Act of Monopolies*, in dem alle Patente außer solchen auf neue, technische Erfindungen für ungültig erklärt wurden. Der einzige, noch mit vergleichbaren Missständen belastete Markt war der für Bücher und Druckwerke; hier setzte das *Statute of Anne* in Wahrheit an. Allerdings scheinen seine Auswirkungen relativ gering gewesen zu sein, die Verleger ignorierten das Statut in ihrem Geschäftsbetrieb offenbar weitgehend. So wurden die Rechte an den Werken Shakespeares, die nach dem Gesetzestext bereits seit 1731 ausgelaufen waren, noch 1768 an den Meistbietenden versteigert.

Dass der Werkautor im *Statute of Anne* als der erste *owner* des ausschließlichen Druckrechtes bestimmt wurde, wird häufig mit der erstmals 1689 anonym veröffentlichten Arbeitstheorie John Lockes³⁴ in Verbindung gebracht³⁵. Danach erwirbt der Mensch Rechte an Sachen durch aneignende Be- und Verarbeitung. Als grundlegendes Beispiele bringt Locke das Einsammeln von Früchten eines herrenlosen Baums; Elemente wie Tausch, Geld oder Vererbung führt er erst am Ende seiner Argumentationskette ein und Rechte an unkörperlichen Sachen spielen bei ihm gar keine Rolle. Für den Übergang von einem feudal Wirtschaftssystem zu einem kapitalistisch geprägtem waren seine Überlegungen bahnbrechend, als Legitimationsgrundlage für eine moderne und komplexe Gesellschaft erweisen sie sich freilich als lückenhaft. Gerade für die Rechte von Autoren liefern sie bestenfalls einen Denkanstoß, aber keine Lösung. Die eigentumsrechtliche Zuordnung von körperlichen Sachen liegt insofern auf der Hand, als der unmittelbare materielle Zugriff des einen Individuums auf eine Sache - schon der "Natur der Sache" nach - den eines anderen ausschließt. Zur Begründung vergleichbarer Rechte am unkörperlichen Werk reicht die Bearbeitung von Papier durch Beschreiben aber eben nicht aus³⁶, insbesondere auch, weil, ganz abgesehen vom reinen Abschreiben, kaum eigentümliche geistige Schöpfungen denkbar sind, in die nicht das aus anderen Werken erworbene Vorwissen einfließt. Das Grundproblem ist also, wie weit der Rechtsschutz überhaupt gehen soll. Ein reines Verlegerrecht benachteiligt Autoren, ein zu starker Schutz von Autoren, der z.B. nicht nur den konkreten Text sondern auch die darin entwickelten Ideen umfasst, behindert die Gesellschaft insgesamt. Dafür wo diese Trennlinie zu ziehen ist, gibt die Arbeitstheorie allerdings wenig her und das *Statute of Anne* wich einer Lösung dieses Problems eher aus, wohl auch weil wohl kaum nachhaltiges Interesse daran bestand, das bisherige System der Inhaltskontrolle veröffentlichter Werke vollständig abzuschaffen.

6. Die entscheidende Wende hin zu einem Urheberpersönlichkeitsrecht kam erst mit Immanuel Kant. Er wandte sich explizit gegen den Nachdruck von Büchern³⁷ ohne Zustimmung des jeweiligen Autors und kritisierte dabei vorrangig die Ansicht, das Eigentum an einem körperlichen Werkstück würde die

³³ E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 95.

³⁴ J. Locke, *Zwei Abhandlungen über die Regierung*, 7. Auflage Frankfurt a. M. 1998, II, § 25.

³⁵ Vgl. dazu E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 82 m.w.N.

³⁶ Dies arbeitet E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 79 ff recht treffend heraus.

³⁷ I. Kant, *Von der Unrechtmäßigkeit des Büchnernachdrucks*, Berlinische Monatsschrift 5/1785, S. 403 ff. nachgedruckt in UFITA 106/1987, S. 145 ff.

Berechtigung zu dessen Vervielfältigung und Verbreitung einschließen, doch wandte er sich auch prinzipiell gegen die Auffassung, die Verlegertätigkeit sei mit dem Gebrauch eines Eigentumsrechts als solchem vergleichbar. Er unterschied dann zwischen einem persönlichem Recht (also einer schuldrechtlichen Befugnis), die der Autor einem Verleger auf Vertragsbasis überlassen könne und welches dann diesem zustehe und einem unveräußerlichen *ius privatissimum*, das in der Berechtigung des Autors bestehe, über sein Werk mit dem Publikum, der Öffentlichkeit zu kommunizieren und das ausschließliche Entscheidungsrecht über Art, Umfang und etwaige Änderungen der Verbreitung begründete.

Kant kommt zu dieser Differenzierung über einen interessanten Ansatz, denn er geht zunächst nicht von einem Schriftstück, Manuskript oder Buch, also einem körperlichem Gegenstand aus, sondern von der Rede, die der Autor an seine Leser halte. Die gesprochene Rede als Handlung eines Individuums kann unabhängig von diesem nicht existieren, sie sei ihm und nur ihm für immer zugeordnet und in diesem Sinne unveräußerlich. Die Schriftform und damit auch das gedruckte Buch ist also sozusagen "nur" eine Verkörperung dieser Rede und bleibt dieser in ihrem Schicksal rechtlich untergeordnet³⁸. Kant vertrat damit also eine recht extreme Position zugunsten des Autors.

Johann Gottlieb von Fichte³⁹ entwickelte diese Argumentation einerseits weiter, andererseits relativierte er sie auch und machte sie so konsensfähig⁴⁰. Er unterschied am Beispiel des Buches drei Komponenten: einerseits die Verkörperung eines Werkes, also das bedruckte Papier, andererseits dessen Inhalt, die Gedanken und Ideen, die ein Buch vorträgt sowie zuletzt deren konkrete Form, die Art und Weise in der sie der Autor vorträgt, also die Worte, Wendungen und Formulierungen die er benutzt. Die Verkörperung, das Buch als greifbarer Gegenstand sei durch den Verkauf in das Eigentum eines anderen übertragbar. Der gedankliche Inhalt dagegen ginge mit der Veröffentlichung in eine Art Gemeingut über, da jeder Leser ihn in seine eigene Ideenwelt integrieren konnte. Die Form jedoch, die Zeichen, mittels welcher ein Gedanke vorgetragen werde sei etwas, das niemand sich ohne Veränderung zueignen könne, sie bleibe auf immer ausschließliches Eigentum des Verfassers. Daraus folgte und forderte Fichte erstens, in persönlichkeitsrechtlicher Hinsicht, dass dem Autor niemand dieses (geistige) Eigentum⁴¹ absprechen dürfe, und zweitens, ebenfalls in persönlichkeitsrechtlicher Hinsicht, allerdings mit direkter vermögensrechtlicher Wirkung, das Recht zu verhindern, dass irgendjemand Eingriffe in dieses Eigentumsrecht täte. Demzufolge könne der Verleger auch durch Vertrag nicht mehr als ein Nutzungsrecht erwerben, welches ihm, im Namen und Auftrag des Verfassers und zu dessen Bedingungen zur beschränkten Vervielfältigung und Verbreitung berechtige.

Damit bereitet Fichte den Boden für jenen dualistischen Ansatz, der die persönlichkeits- und vermögensrechtliche Seite als Einheit sieht und das Urheberrecht bis heute prägt. Erst die umfassende Verbreitung der Technik des Buchdrucks und ein völlig neuer Markt, der dadurch entstand, haben zusammen mit der aufklärerischen Vorstellung vom Menschen, der im Zentrum der Schöpfung selbst schöpferisch tätig ist, die herrschende Urheberrechtsordnung ermöglicht⁴².

³⁸ Vgl. E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 343 f.

³⁹ J.G. Fichte, *Beweis der Unrechtmäßigkeit des Büchernachdrucks. Ein Räsonnement und eine Parabel.*, Berliner Monstsschriften 21/1793, S. 443 ff.

⁴⁰ E. Höffner, *Geschichte und Wesen des Urheberrechts*, Band I cit., S. 368 ff.

⁴¹ Terminologisch ist die Anlehnung ans Eigentum körperlicher Sachen hier also eher eine geistige Brücke, die eine Analogie zum sachenrechtlichen Eigentum gerade nicht sucht.

⁴² M. Reh binder, *Urheberrecht*, 16. Aufl., München 2010, S. 7.

PRINCIPEN OM GOD SED, SÄRSKILT I NAMNANGIVELSE- ELLER PATERNITETSRÄTTEN

THE LEGAL PRINCIPLE OF FAIR PRACTICE, ESPECIALLY IN THE PATERNITY RIGHT

ALFRED STRENG

Dr. Sc. (Econ. Law), Pol. Lic., Researcher, University of Vaasa, Finland
Street Number Wolffskavägen 34, 65200 Vasa, Finland (Pb 700, 65101 Vasa, Finland)
alfred.streng@uva.fi; <http://old-www.uvasa.fi/talousoikeus/henkilokunta/streng/>

Keywords: *Copyright, paternity, fair practice, legal norm, moral norm*

Abstract: *The principle of fair practice can be seen as both a moral and a legal norm. The paternity right implies that the name of the author should be stated when one of his or her works is made available to the public and especially when a work is performed to the public in a manner required by fair practice. Where the paternity right is concerned, the requirement of fair practice applies to all types of copyright-protected works and the case law in different areas of copyright can be applied to the corresponding areas where a digital environment is involved.*

1. Generellt

Den rättsliga principen om god sed har sitt ursprung i den romerska lagen där det fanns en rättsregel enligt vilken en debenture som inte var i enlighet med god sed (contra bonos mores) uppfattades som ogiltig.

Principen om god sed kan uppfattas som både en moral- och en rättsnorm. Plikten att följa en moralnorm kan basera sig på en allmän uppfattning i samhället om vad som är ett rätt eller uppskattat beteende. Plikten att följa en rättsnorm baserar sig på rättssystemets åläggande att handla i enlighet med lagen. Ett av de grundläggande elementen i ett utvecklat rättssystem är att motiveringarna för domstolsbesluten bör basera sig på lagen.¹ Normativt baserade beslut, hör till uppgifterna för ett utvecklat rättssystem. Då lagreglerna inte alltid föreskriver de motiveringar som krävs, finns det rättsprinciper som kan styra tolkningen av lagreglerna och, så att säga, fylla de luckor som lagreglerna lämnat öppna. Rättsprinciperna har så kallat institutionellt stöd. Förekomsten av en specifik lagregel kan motiveras genom att hänvisa till tidigare domstolsbeslut samt till konstitutionella och legislativa principer. Det finns ingen allmän kontroll genom vilken man kunde uppskatta validiteten av rättsprinciper i vissa specifika fall. I motsats till normala rättsregler är rättsprinciperna inte giltiga eller ogiltiga. Den rådande lagen utesluter dock inte i sig moralnormer. Enligt von Wright kan inte ens moralnormer identifieras med det totala antalet rättsliga föreskrifter som kanske stöder dem². Det faktum att rättsnormer och moralnormer har

¹ Se Strömholm 1966: II:1: 34.

² Se von Wright 1963: 12–13.

liknande kännetecken gör dem inte i sig identiska eller reducerar inte den ena typen av normer till en kategori inom den andra.

I Finland har rättshandlingar som ansetts strida mot principen om god sed förklarats ogiltiga redan innan specifika rättsregler förekommit i lagen i fråga. I rättslitteraturen har rättshandlingar som stått i konflikt med principen om god sed uppfattats som tillhörande de mest nedvärderade typerna av otillbörliga handlingar. Otillbörligheten i en rättshandling på grund av att den står i konflikt med principen om god sed, kan även anses bero på att rättshandlingen ifråga är klart illegal. Denna syn kan godkännas, särskilt om begreppen ”lag” och ”lagenlighet” uppfattas som att omfatta alla normer och rättsprinciper, också de som uttryckligen inte ingår i den skrivna lagen. En rättshandling som står i konflikt med principen om god sed skulle därmed kunna anses strida mot vad tillhör den allmänna rättsordningen.

Enligt *Aarnio* och *Peczenik* kan principen om god sed karaktäriseras såsom tillhörande sedvanerätten. Sedvanerätten kan omfatta sådana etablerade handlingssätt som berör allmänheten generellt, eller något specifikt område som inte explicit är uttryckt i lagen. Watson för fram åsikten att sedvanerätten är vanligast inom områden där lagen tenderar att vara minst teoretisk. Men lagen kräver dock teoretiska utgångspunkter, oavsett om dessa utgångspunkter alltid är implicita. Följaktligen, för att en sedvana skall betraktas som lag i det västerländska rättssystemet, krävs det mer än bara ”vana”, fastän vanan ifråga skulle vara allmänt och länge utbredd. Det är här alltså fråga om att man bör särskilja det som ”är” från hur det ”bör vara”. Enligt *Pöyhönen* kan man inte värdera god sed och sedvana juridiskt som om rådande sedvana och god sed skulle ha samma innebörd.³ Sedvanan får inte samma juridiska innebörd som god sed enbart av den orsaken att den används allmänt. Mer väsentligt är, att sedvanan utmärker sig genom att avspegla sakenligt och jämbördigt olika parter intressen. En befäst sedvana kan sålunda representera den ena partens intressen på ett sådant sätt att man inte kan likställa dem med god sed.

Sedvanerätt kan å ena sidan ha sitt ursprung i ett handlingssätt i samhället som med tiden blivit så enhetligt att det kan kategoriseras som sedvanerätt. Å andra sidan kan konsistenta domstolsbeslut i liknande fall klassificeras som sedvanerätt när de kategoriseras som rättspraxis.

Från ett brett perspektiv kan regelbundenheter i olika former av mänskliga verksamheter uppfattas som sedvanerätt. Det faktum att ett handlingssätt är regelbundet och allmänt accepterat, implicit eller explicit, gör det dock inte nödvändigtvis till en sedvana som skall kategoriseras som tillhörande sedvanerätten. Från ett mera snävt perspektiv omfattar sedvanerätten således uttryckligen sådana handlingsnormer som berör hur regler följs inom något specifikt rättsområde.

Effektiviteten i sedvanerättsnormer kan vara beroende av i vilken grad domstolar hänvisar till sedvanerätten ifråga i sina motiveringar. All sedvanerätt har inte samma validitet. Sedvanerätten kan även anses omfatta delar av starka, svaga eller tillåtna rättskällor.⁴ Följaktligen skall inte sedvanerätten ses som en helt objektiv rättskälla. Till exempel krävs det vid beslut om huruvida ett handlingssätt är i enlighet med god sed alltid att de specifika omständigheterna för situationen ifråga beaktas, såväl platsen som de berörda parterna. Enligt *Kaisto*⁵ kan det vid frågan om den konkreta tillämpningen av rättsprincipen om god sed gälla att lagstiftaren lämnar den öppen för domarens fria bedömning. Därtill är de uppfattningar om vad som är god sed i det specifika berörda området ifråga av stor betydelse när beslutet skall göras.

När en rättsregel uttryckligen är oklar vad gäller skäligheten i en rättshandling, är det domstolen som skall avgöra om rättshandlingen ifråga är i enlighet med principen om god sed. En

³ Se t.ex. *Aarnio* 1989: 220, *Peczenik* 1988: 296. Se även *Watson* 1984: 561–562 och *Pöyhönen* 1999:98.

⁴ Se *Aarnio* 1989: 220 och *Peczenik* 1988: 296. Se dock även *Mähönen* 1995: 125–139, *Nuotio* 2004: 1267–1291 och *Pöyhönen* 1999: 198.

⁵ Se *Kaisto* 2005: 155.

rättshandling som ses som ogiltig utgående från principen om god sed behöver dock inte vara moraliskt förkastlig, det räcker med att domstolen anser att den står i konflikt med vad man på basen av sunt förnuft kan uppfatta som god sed. Det är här inte av betydelse huruvida förövaren är medveten om att rättshandlingen står i konflikt med principen om god sed, det räcker med att rättshandlingen ifråga inte är i enlighet med principen om god sed från en objektiv synvinkel. Alla gånger behöver man inte ens ytterligare motivera principen om god sed, det förväntas eller antas helt enkelt att principen åtföljs.

I förmögenhetsrätten har även begreppet stridande mot god sed sedan länge varit av betydelse, trots att det i lagen inte förekommer någon allmän regel om rättshandlingen stridande mot god sed. På en allmän nivå är det svårt att definiera vad för slags sed som är en god sed eller stridande mot god sed. Man kan dock nämna exempel på hurudana rättshandlingar som ansetts eller skulle anses vara stridande mot god sed. Stridande mot god sed kan som en allmän rättsprincip forma en gräns för t.ex. avtalsfriheten. Vissa bestämmelser för stridande mot god sed har uppställts: a) rättshandlingen eller dess villkor är som sådan stridande mot god sed, dvs. enligt allmänna rättsprinciper, b) rättshandlingen har fått till stånd på ett sätt, som kan anses vara stridande mot god sed, c) motivet för utförandet av rättshandlingen är stridande mot god sed eller d) målet för rättshandlingen är avsett att användas för en verksamhet som kan anses för stridande mot god sed. Särskilt begreppet stridande mot god sed har uppfattats vara en ren moralnorm. Begreppet god sed är föränderligt, och en fråga som lämnar rum för tolkning. Det är fråga om ett begrepp som är beroende av flera omständigheter, speciellt varje tids värde- och moraluppfattningar. Å ena sidan kan man anta att ett handlingssätt som majoriteten av befolkningen anser som gott också uppfyller kraven på god sed, men å andra sidan är den rådande uppfattningen hos majoriteten av befolkningen inte nödvändigtvis ett tillräckligt berättigande för validiteten av en moralnorm. Dock kan man ju enligt Niemi hävda att lagen uttryckligen skall tolkas utgående från ett beteende som medborgarna uppfattar vara i enlighet med ett sunt förnuft i konkreta situationer, eller enligt vad man kan förvänta sig av en ärlig och ärbär medborgare.⁶

2. God sed inom olika rättsområden

I finsk rättslitteratur har man ansett, att i rättsliga förhållanden skall god sed följas och att stadgandet om god sed är i kraft som en allmän rättsprincip, fastän det inte förekommer något allmänt stadgande i lagen.⁷ Man har inte särskilt ofta hänvisat till den allmänna principen om god sed eller till stridande mot god sed i rättspraxis, utan ofta stött sig på något annat stadgande.

Numera förekommer specialstadganden om god sed på ett flertal rättsområden. Principen om god sed hänför sig i första hand till avtalsförhållanden, men god sed sträcker sig till andra områden i civilrätten, såsom exempelvis immaterialrätten. Det är omöjligt att definiera god sed allmängiltigt, emedan fråga är om en generalklausul (flexibla rättsnorm), vars innebörd varierar branschvis.⁸

3. God sed i upphovsrätten, särskilt ideella rätten

Principen om god sed förekommer inom så gott som alla områden av immaterialrätten. Inom upphovsrätten förekommer principen om god sed uttryckligen i paternitetsrätten. Det allmänna stadgandet om paternitets- eller namnangivelserätten ingår i 3 § 1 mom. upphovsrättslagen enligt vilken upphovsmannen skall anges på det sätt som god sed kräver. Denna skyldighet att namnge upphovsmannen bör följas då man framställer exemplar av verket eller då verket helt eller delvis

⁶ Se Niemi 1998: 529.

⁷ Se Saarnilehto 1993: 2, Saarnilehto 2005: 40, 59, 135–137, 177, Ämmälä 1993: 5 och Ämmälä 2001: 123.

⁸ Se Tolonen 2003: 200 och Pohjonen 1993: 138.

görs tillgängligt för allmänheten. Denna lagregel kompletteras i Danmark, Norge och Sverige av 11 § 2 momentet URL, som stadgar att när ett verk återges offentligt, skall källan anges i den omfattning, och på det sätt god sed kräver. I Finland gäller efter harmoniseringen att när, i enlighet med inskränkingsbestämmelserna i 2 kapitlet upphovsrättslagen, ett verk framställs eller görs tillgängligt för allmänheten, förutom källan även upphovsmannens namn skall anges i den omfattning och på det sätt som god sed kräver. Samma regel tillämpas även då utnyttjande av verket sker på basen av bestämmelserna om avtalslicens.⁹

Principen om god sed förekommer också i citaträtten, artikel 10(1) BK, artikel 5(3) d Infosoc-direktivet och 22 § nordiska upphovsrättslagarna, enligt vilka citat får göras ur offentliggjorda verk i överensstämmelse med god sed och i den omfattning som motiveras av ändamålet. Direktivet föreskriver dessutom att namn och källa skall anges om detta inte visar sig omöjligt, men de nordiska länderna har kvarhållit uttrycket god sed.

Auktorrättskommitténs goda sed-formulering kan härledas från tankegången att bl.a. rättsläget och praxis inom det upphovsrättsliga området snabbt förändras och lagen bör ha möjlighet att följa med utan omarbetningar. Uttrycket ”god sed” uppfyller dessa förväntningar, emedan den är normativ eller ett uttryck som förutsätter värdering. Detta uttryck ges betydelseinnehåll i varje ny tillämpningssituation. Uttryckets innehåll är beroende av många saker, såsom de värderingar och moraluppfattningar som råder vid tidpunkten. Ordalydelsen i uttrycket ”god sed” ger tillämparen av lagen mycket vidare tolkningsmöjligheter än direktivets uttryck ”om inte detta visar sig omöjligt”. ”God sed” möjliggör även en sådan tolkning, att namnet och källan kan förbli onämnda, fastän nämnandet av dem inte är omöjligt. Man kan tala om god sed sålunda endast under de förutsättningar, att det att namnet och källan inte nämns får ett allmänt godkännande i ifrågavarande fall. En rådande sed i någon bransch är inte en god sed, om inte den får allmänt godkännande, varom i meningsskiljaktigheter avgörs i sista hand i domstolarna. Namn- och källangivelsekravets omfattning och innehåll, som grundar sig på god sed, varierar förstärligt enligt olika användningssätt och -syfte för materialet ifråga. Analog och digital teknik tillåter väldigt olika sätt att utforma namn- och källangivelse. Till den digitala tekniken hör ändå inte sådana begränsningar, som ofta godtogs i analogt material.

Enligt rådande uppfattning är principen om god sed eller principen som förutsätter följande av god sed gällande i civilrätten som en allmän rättsprincip, fastän det inte finns något allmänt stadgande i lagen. Specialstadgandena om god sed innefattas i 3 § 1 mom., 11 § 2 mom. och 22 § upphovsrättslagen, såsom ovan konstaterats. Utanför dessa stadganden kan man i upphovsrättsliga förhållanden tillämpa civilrättslig allmän rättsprincip om att följa god sed. Enligt denna kan man tillämpa allmän rättsprincip om god sed i samband med respekträtten, fastän principen inte explicit är uttryckt i 3 § 2 mom. upphovsrättslagen. Användaren skall iaktta god sed så att han inte kränker upphovsmannens litterära eller konstnärliga egenart eller anseende. Han skall exempelvis inte ändra verk så, att ovan nämnd kränkning sker och inte heller tillgängliggöra verket för allmänheten i sådan form eller i sådant sammanhang att det gör intrång i upphovsmannens respekträtt. Användningen av ett upphovsrättsligt skyddat verk bör ske enligt god sed. Ett förfarande i enlighet med god sed uppfyller i detta sammanhang även de krav som ställs på uppfyllandet av lojalitetsprincipen.

Generalklausulen ingår i 3 § 1 mom. upphovsrättslagen, som gäller paternitetsrätten (namnangivelse-rätten). Specialstadgandet om god sed och namnangivelse-rätten finns i 11 § 2 mom. upphovsrättslagen. Dessutom ingår stadgandet om god sed i 22 § upphovsrättslagen, som gäller citaträtten. I andra situationer kan man tillämpa den civilrättsliga allmänna rättsprincipen om god

⁹ Se KB 2002: 5: 50–53, 55–56, 58, RP 28/2004: 32, 35, 36, sv. prop. 2004/05:110: 84–88, Forslag til Lov om ændring av ophavsretsloven L 17, 19, Ot.prp.nr.46 2004–2005.

sed. Med denna kartläggning skapas ramar för senare framläggning av ideella rättigheter, där man behandlar namnangivelserätten och respekträtten samt vissa inskränkningar i upphovsrätten, närmast citaträtten, och i sammandrag namn- och källangivelseskyldigheten.

4. Paternitetsrätten

4.1. Allmänt om paternitetsrätten

Upphovsmannens namn skall anges på det sätt som god sed kräver då man utnyttjar ett verk på en av de i 2 § upphovsrättslagen nämnda befogenheterna och i enlighet med inskränkningarna i upphovsrätten samt bestämmelser om avtalslicens i 2 kapitlet. Stadgandet i 11 § 2 mom. upphovsrättslagen förutsätter, att förutom upphovsmannens namn skall källan anges, om användningen grundar sig på inskränkningsreglerna i upphovsrätten eller bestämmelserna om avtalslicens. Med stöd av denna kan man särskilja namnangivelseskyldigheten och källangivelseskyldigheten. Skyldigheter i samband med namnangivelserätten bör följas oberoende av om användningen av verket är lovligt eller olovligt. Vid plagiat kan det föreligga intrång inte enbart i de ekonomiska rättigheterna, utan också i upphovsmannens ideella intressen ligger att det riktiga upphovsmannaförhållandet anges.

Man skall ange upphovsmannen på exemplar av verket, där det överhuvudtaget är möjligt och där namnangivelsen inte kommer att verka orimligt förstörande på verket. Enligt *Lund* kan det vara fråga om vanskelighet (svårighet) att namnge på konstindustriella produkter och störande eller egendomligt att ange upphovsmannens namn vid gudstjänster eller begravingar. I rättslitteraturen framgår det även att namnangivelse av upphovsmannen är inte i praktiken alltid nödvändigt, såsom bakgrundsmusik vid restauranger, caféer etc. och inte heller i alla situationer möjligt, dvs. omöjligt. Att frånga namnangivelse kan enligt *Kivimäki* vara vanligt vid byggnadskonst, men inte vad gäller dess ritningar. Man har ytterligare i rättslitteraturen ansett att det kan medföra praktiska svårigheter, såsom konstindustriella produkter. Enligt Auktorrättskommittén skulle det verka störande att ange upphovsmannen, t.ex. musikutförande vid gudstjänst eller av tekniska skäl kan det vara svårt att tillgodose upphovsmannens anspråk att anges på exemplar av verk, exempelvis i fråga om konstindustriella glasprodukter.¹⁰

Eftersom substansen i god sed kan påstås variera från bransch till bransch och i enlighet med de specifika omständigheterna för fallet ifråga, är det rättspraxis som i långt kommit att avgöra vad som avses med principen om god sed i paternitetsrätten. Nedan följer en klarläggning av namnangivelserätten med avseende å verkstyper, emedan man i rättslitteraturen ifrågasatt huruvida rätten kan vara explicit eller implicit eftergiven.

4.2. Bildkonstverk

Bildkonst omfattar sådana framställningar där bilden är framställningens egentliga syfte och där det inte ingår något nyttosyfte, såsom fallet är gällande byggnadskonst och brukskonst.

I rättsfallet "Gunilla Rudling", där HD ansåg att avlägsnande av en konstnärs namnlogotype från ett antal i stor upplaga framställda färgreproduktioner av målningar, vilka köpts i handeln och utnyttjas för biografreklam, stod i strid med 3 § URL. Färgreproduktionerna hade beskurits och bilderna delats och placerats i ett montage utanför en porrbio.

¹⁰ Se *Kivimäki* 1966: 39–40. Se även SOU 1956: 25: 116.

Som en grundprincip kan man här anta att upphovsmannens namn skall anges i alla fall där inte störande och tekniska orsaker eller praktiska svårigheter kräver motsatsen i enlighet med 3 § 1 mom. URL. Ett filmbolag, som köpt sju affischer, utgörande reproduktioner av konstverk som utförts av upphovsmannen *Gunilla Rudling*, skulle använda affischerna som reklam för pornografiska filmer efter att man ändrat dem. Reproduktionerna av *G. Rudlings* affischer, där namnlogon hade skurits bort, kränkte hennes paternitetsrätt och stred mot god sed. Till upphovsmannens ideella rätt hör att han respektive hon själv bestämmer om var på verket och hur det namnges samt även huruvida namnet överhuvudtaget skall nämnas. Namnangivelsen har inte ansetts ovillkorlig, men den bör ske enligt god sed. Man har också ansett att namnet lämnas bort endast om det är enligt god sed. Borttagande kan otvivelaktigt anses som stridande mot god sed. Reproduktionerna i färgtryck, eller s.k. affischer, hade tryckts i stor upplaga för försäljning till allmänheten i olika länder. I detta fall var antalet beskurna affischer inte större än sju, men tillämpningen av 3 § 1 mom. upphovsrättslagen är inte beroende av verkets mängd. De beskurna affischerna hade tillgängliggjorts för allmänheten, både i entrén till biografen och i montaget utanför en biograf. Man kan anse att denna handling var stridande mot god sed och minskade upphovsmannens försäljning av sina verk genom att den reklam som offentliggörandet av affischerna kunnat medföra, nu negligerades. Därtill kan verkningarna yppa sig i form av att upphovsmannen får sämre ekonomiska villkor i förhållande till förlag eller motsvarande instanser. Detta kan ske på grund av att allmänheten inte får korrekta uppgifter om vem som är upphovsman, en försummelse av informationsplikten.

Textiltryck, konstvävnad, mosaik och vissa typer av glas- och keramikarbeten samt smyckeskonst hänförs till alster av bildkonst. Fråga i följande fall är huruvida man på smycken ingraverar upphovsmannens namn.

I fallet HD 1992: 63 "Kaleva Koru", anförde Högsta Domstolen att praxis var att ange upphovsmannens namn på smycken varierar. Namnet på välkända konstnärer associeras vanligtvis till en viss typ av smycken eller anges åtminstone på smyckets förpackning. I vissa fall gäller att namnet på upphovsmännen till smycken enbart anges på förpackningarna. Avtalet mellan parterna i fallet förutsatte inte att namnet på upphovsmännen skulle anges på varje enskilt smycke. Upphovsmannen ansågs därmed inte ha rätt till ersättning på grund av upphovsrättsligt intrång.

I fallet har man tagit fasta på att då det gäller att igenkänna upphovsmannen till smycket är den konstnärliga utformningen av smycket av större vikt än själva namnet på upphovsmannen. Detta kan gälla för redan etablerade och välkända konstnärer, men för nya förmågor kan det vara svårare att göra sig kända, ifall inte konsumenterna får klar information om vem som är upphovsman till verket, speciellt om HD i motiveringarna till domslutet konstaterat, att det inte i branschen (affärerna) var ett uteslutande eller ens ett vedertaget bruk. Man har i motiveringarna tagit fasta på branschsed. Men variationer förekommer i branschen. Särdeles etablerade konstnärers namn fogas i allmänhet på varje verk, men det är inte ett konsekvent förfarande. I branscher förekommer också att man oberoende av ryktbarhet endast anger upphovsmannen på förpackningarna.

4.3. Litterära verk

Till de litterära verken hör det egentliga skönlitterära området, vare sig det är fråga om en roman eller en novell, lyrik eller någon annan litteraturform med litterär syftning. Även skolböcker omfattas av det litterära verksamhetsområdet.

I ett finskt rättsfall HD 2005: 43 "Lärobok i språk", som gällde en lärobok omfattande en skild textdel och ordlista. Ett företag hade utan upphovsrättsinnehavarnas medgivande kopierat ordlistan på maskinläsbara disketter och börjat marknadsföra disketterna. Högsta Domstolen ansåg att företaget hade kränkt upphovsrättsinnehavarnas paternitetsrätt.

I rättsfallet "Lärobok i språk" hade ett företag marknadsfört litterära verk (skolböcker) utan att namnge upphovsmännen på maskinläsbara disketter eller i marknadsföringen av dem, vilket är att anse som stridande mot god sed. God sed hade förutsatt att man även nämnt upphovsmännen till de litterära verken, emedan disketterna innehöll ordlistor, som var en del av de litterära verken. Upphovsrättsligt skydd omfattas av såväl hela som delar av verk, såvida de uppfyller verkshöjdskraven, vilket HD tog ställning till i sina motiv.

I enlighet med 3 § 1 mom. upphovsrättslagen har upphovsmannen rätt att bli angiven med sitt namn då exemplar av ett verk framställs eller verket helt eller delvis görs tillgängligt för allmänheten på det sätt som god sed kräver. Namngivelseskyldigheten är inte ovillkorlig, utan man bör ange upphovsmannens namn såsom god sed kräver. Avsikten att använda objektet, de olagligt framställda kopiorna, utan angivelse av upphovsmannens namn, i en aktivitet som är i konflikt med principen om god sed skadade upphovsmannen, emedan allmänheten inte kunde få vetskap om vem som hade skapat verket.

HD fastställde i sin dom att intrång skett i namngivelserätten enligt 3 § 1 mom. URL, varmed ersättning i enlighet med 57 § 2 mom. upphovsrättslagen skulle erläggas åt upphovsmännen för intrång i namngivelserätten.

I avgörandet togs ställning till otillbörligt förfarande i näringsverksamhet, men HD konstaterade, att innehavarna till de ekonomiska rättigheterna, bokförlagen, inte har specificerat hurudan ekonomisk förlust med marknadsstörningar och avbrott i konsumentrelationerna de åsamkats genom det svarande företags handlande. Av denna anledning ansåg HD att ersättning inte kunde utdömas. Man har inte erhållit HD:s ställningstagande, huruvida skada förorsakad av marknadsstörningar enligt lagen om otillbörligt förfarande i näringsverksamhet kunde tillämpas vid intrång i upphovsrättens ekonomiska rättigheter. Däremot framförs här synpunkter på att intrång i de ideella rättigheterna kan motiveras med argument eller parametrar som gjorts gällande vid otillbörligt förfarande i näringsverksamhet. Händelseförloppet var, att företaget hade marknadsfört de digitala litterära verken via sin webbsida på Internet, varifrån man även kunde köpa dem. På grund av att upphovsmännen inte hade namngivits och förbundits vid sina verk hade de inte kunnat skörda frukterna av sitt eget arbete. Däremot hade företaget "seglat under fel flagg" och njutit av reklam med falska uppgifter. Företagets ageranden kunde ha bidragit till att upphovsmännens namn inte blir vida känt och att de eventuellt inte hade lika goda förutsättningar att erhålla ekonomiskt understöd i framtiden, då försäljningen av originalverkens upplagor minskat, detta p.g.a. att renommé-uppbyggelsen försvagades här. Företaget hade i sin verksamhet inte handlat förenligt med god sed och visat upphovsmännen brister enligt lojalitetsprincipen, dvs. man hade förbisett upphovsmännens fördel och behov genom att underlåta att nämna deras namn på disketterna och i marknadsföringen enligt 3 § 1 mom. upphovsrättslagen.

Till exempel utgivningen av en bok har uppfattats som ett utnyttjande som kräver att namnen på alla upphovsmän anges, då det är viktigt att någon sammanblandning av upphovsmännen inte sker. Det har ansetts att namnet på upphovsmannen däremot inte behöver anges vid reklam, om det saknar betydelse för upphovsmannen eller om det är störande, såsom till exempel på restauranger och vid kyrkliga förrättningar. Ett visst mått av flexibilitet har alltså krävts vid angivandet av upphovsmannens namn. I ovannämnda fall var namngivelse vid reklam något som upphovsmännen synbarligen inte motsatt sig, snarare förväntat sig.

Det är av ingen relevans för paternitetsrätten i vilken omfattning ett upphovsrättsskyddat verk används så länge det kan identifieras som skapat av en viss upphovsman (1 § URL). Det är inte heller av betydelse huruvida verket görs tillgängligt för allmänheten i en bearbetad version (4 § 1 mom. URL), med en ny teknik eller i ett nytt medium så länge som upphovsmannen till verket ifråga kan anknytas till verket. Att ett verk mångfaldigas i en form som har en likhet med originalverket, betyder inte att upphovsmannens namn inte skulle behöva anges. Skyldigheten att

ange upphovsmannens namn i enlighet med god sed är inte heller beroende av huruvida utnyttjandet av verket är lagenligt eller ej eller i enlighet med någon lagregel om undantag eller begränsning.¹¹

Utöver det skönlitterära omfattar det litterära verksbegreppet också beskrivande framställningar och rapporter som uppfyller verkshöjdskraven.

I rättsfallet Vestre Landsret B-0102-93 "Biolog", gällde saken en fast anställd biolog, som krävde att hennes namnangivelse rätt skulle tas i beaktande i samband med en rapport som hon gjort i ett anställningsförhållande i en kommun. Med hänvisning till god sed ansåg rätten det berättigat att biologens namn skulle anges på alla exemplar av rapporten. Rapporten ansågs inte vara av sådan karaktär, att den omfattades av 9 § URL, som reglerar att lagar och förordningar samt beslut och yttranden av myndighet eller annat offentligt organ inte är föremål för upphovsrätt, utan biologens rapport befanns vara ett upphovsrättsligt verk enligt 1 § URL. Man torde kunna anse att avgörande för namnangivelseplikten var, att det, åtminstone var en sedvana i andra kommuner att upphovsmannens namn angavs. Fråga kan även vara om skydd av den svagare parten, upphovsmannen, att lojalitetsprincipen skall beaktas.

4.4. Musikaliska verk

Ett musikaliskt verk har karaktären av ett musikaliskt verk oavsett i vilken form det framträder, dvs. i form av notskrift, som inspelning eller som ett offentligt framförande.

Det har inte ansetts tillåtet att, på ett eller annat sätt, ta bort upphovsmannens namn från verk som görs tillgängliga för och framförs för allmänheten. Till exempel förutsätter principen om god sed att namnen på upphovsmannen och den utövande konstnären anges när deras musikverk spelas såväl i analoga som digitala media. Detta krav kan även uppfyllas genom att namnen på upphovsmannen och den utövande konstnären anges till exempel i skriven form i programkolumner i tidningar eller i digital form som diverse meddelande. Som följande fall visar kan det dock vara svårt att bedöma när kravet på god sed uppfylls.

Upphovsrättsrådet i Finland ombads ta ställning i ett fall 1992:13 angående radiostation B:s sändningar av klassisk musik

Enligt part A sände radiostation B musikverk på ett sådant sätt att det förblev oklart när ett musikaliskt verk var slut och det följande började. Därtill blandades musiksändningarna med reklam. A menade att detta stred mot upphovsmannens ekonomiska och ideella rättigheter, då det var omöjligt att veta vems musikverk som spelades och då detta sätt minskade respekten för klassisk musik och degraderade den till en simpel vara.

Företrädare för radiostationen B menade att upphovsmännens namn alltid nämnts när deras verk sändes och att musikverk aldrig blandats med reklam. B var överlag av den åsikten att det är svårt för radio-stationer att förmedla programuppgifter till lyssnarna. De vanliga dagstidningarna hade inte publicerat programuppgifterna och radiostationen hade börjat publicera en egen tidning Klassinen Musiikki, för att uttryckligen förmedla programuppgifter åt lyssnarna.

Upphovsrättsrådets åsikt i saken var att principen om god sed förutsätter att kompositörernas och de utövande konstnärernas namn nämns när deras verk spelas. I vissa fall kan detta krav uppfyllas genom att namnen nämns i programkolumner i tidningar. Radiostation B:s verksamhet baserade sig på sändning av klassisk musik och den centrala ställning som de klassiska musikverken hade i dess verksamhet gjorde sitt till att betydelsen av de ideella rättigheterna betonades. Upphovsrättsrådet ansåg att radiostationen B hade nämnt kompositörernas och de utövande konstnärernas namn i enlighet med god sed men i vissa särskilda fall försummat att uppfylla kravet på att nämna namnet

¹¹Se RP 28/2004: 82.

på kompositörerna och de utövande konstnärerna. Radiostationen B ansågs sålunda inte ha gjort intrång i kompositörernas och de utövande konstnärernas ideella rättigheter.

Kravet på god sed ansågs således ha uppfyllts i stort eftersom man vidtagit åtgärder för att förmedla programuppgifterna åt lyssnarna. Det att upphovsmännens namn inte framkom i vissa särskilda fall var inte en tillräcklig grund för att intrång i de ideella rättigheterna skulle ha skett. Ur en helhetssynvinkel var försummelserna så ringa, att man ansåg dem inte utgöra sådana kränkningar, som skulle ge upphov till upphovsrättsliga påföljder.¹² Det normala ansågs således vara att namnen på upphovsmännen angavs. Till det kan man tillägga att det torde förekomma en god sedvana i branschen, emedan det är enligt god sed att namnge upphovsmännen och de utövande konstnärerna i radio och TV¹³. Förpliktelse att ange upphovsmännen och de utövande konstnärerna vid framföranden gäller då det är fråga om ett tillgängliggörande för allmänheten. En tillräcklig grund för intrång är inte att det sker vissa, kanske sporadiska, undantag från en allmän praxis. Man kan anlägga en objektiv måttstock för denna fadäs.

När musikverk framförs live för allmänheten är det oftast ingen tvekan om att namnen på kompositörerna, andra upphovsmän och de utövande konstnärerna nämns i programblad eller i samband med framförandet. Den rådande seden i radio- och andra sändningar har varit att titlarna på en rad verk nämns samtidigt. Likaledes är det vid TV-sändningar och biografspelningar vanligt att en samlad lista av upphovsmän, utövande konstnärer, medarbetare och andra medverkande visas. Enligt *Karhu* är en rådande sed inte alltid ur upphovsrättslig synpunkt en god sed, varmed han exempelvis nämner radions massutnyttjande av lätt musik. Då man spelar musik av den lätta genren har en rådande sed blivit, att man inte i något skede nämner upphovsmännen eller de utövande konstnärerna. Detta förfaringssätt uppfyller inte ens de minimikrav, som förutsätter att man enligt god sed namnger upphovsmännen.¹⁴ Enligt *Koktvedgaard & Levin* har sådan praxis dock ansetts mera som en gest utan större värde än något som skulle ha relevans för rättsinnehavarna.¹⁵ Trots allt, ligger det, förutom i upphovsmännen intresse, även i nuvarande och presumtiva konsumenters intresse att få veta vem som är upphovsmän till ett visst verk.

I de följande danska och svenska rättsfallen tillmättes kravet på god sed i paternitetsrätten dock stort värde.

I ett danskt rättsfall (U 1947: 187 Ö ”Den lille Napoleon”) ansåg domstolen att försummelsen att i samband med en filmspelning inte nämna namnet på kompositören till filmmusiken utgjorde ett intrång i kompositörens namnangivelserätt. Kompositören ansågs ha rätt att få sitt namn nämnt. Det faktum att han hade fått ersättning för sitt kompositionsverk påverkade inte hans rätt att bli nämnd i samband med sitt verk.

Domstolens beslut visar att huvudregeln alltid skall vara att upphovsmännens namn nämns, ifall inte särskilda oöverkomliga hinder förekommer för ett omnämnande. Med detta ställningstagande befrämjade domstolen en sedvanebildning inom branschen. Här ansågs namnangivelsen inte bara vara en värdelös gest, utan försummelsen av namnangivelsen ansågs som stor och stridande mot god sed. Upphovsmännens rätt att bli namngiven i enlighet med 3 § 1 mom. upphovsrättslagen bidrar till att han blir känd för sitt upphovsmannaskap, vilket medför att han kan etablera sig på marknaden och bli konkurrenskraftig med sina verk. Enligt principen om god sed är en handling som förorsakar upphovsmannen skada rättsstridig.

Noterbara synpunkter är dock, såsom även *Schönning* påpekar, att namnangivelserätten är beroende av god sed och inte absolut. Numera förekommer en ovillkorlig skyldighet att ange

¹² Se *Sorvari* 2005: 215.

¹³ Se *Stannow* et al. 2005: 69.

¹⁴ Se *Karhu* 2005: 290 och 2006:299.

¹⁵ Se *Koktvedgaard & Levin* 2003: 138–141 och *Levin* 2011: 162–163.

upphovsmannens namn och källan, då fråga är om artiklar om dagsfrågor. Detta förutsätts av Infosoc-direktivets artikel 5(3) punkt c). Detta stadgande om informationsskyldighet innefattas numera i 23 § 2 mom. upphovsrättslagen. I andra fall gäller skyldigheten att informera om upphovsmannens namn och källan om det är i överensstämmelse med god sed, m.a.o. om man inte kan namnge p.g.a. omöjlighet eller svårighet att uppfylla kraven. I dylika fall kan i rättslitteraturen framförda tankar om att bortlämnande sker enbart om det är enligt god sed eller överenskommelse vara på sin plats. Sedvanan på det enskilda området är av betydelse, men god sed är inte detsamma som varje sedvana eller skick och bruk. Men om sedvanan inte representerar en rimlig och ärbar handling, stämmer den inte överens med kravet på god sed. I och med att utnyttjande av upphovsmannens musikverk förekommit hade utnyttjaren inte beaktat den fördel och det intresse som upphovsmannen skulle ha av att bli namngiven och få den erkänsla som kunde komma honom till del, m.a.o. brister enligt lojalitetsprincipen gentemot upphovsmannen.

I ett liknande fall i Högsta domstolen i Sverige, Stadens löjtnant, var det en rad kända svenska kompositörer som hävdade att deras paternitetsrätt inte beaktades i den omfattning som principen om god sed kräver när deras musik spelades i Sveriges Television (SVT).

Högsta domstolen biföll kompositörernas krav och ansåg att SVT hade brutit mot god sed på området genom att underlåta att namnge upphovsmannen. Upphovsmännens namn skall alltid nämnas så länge det inte är omöjligt på grund av tekniska eller störande orsaker. Högsta domstolen betonade att utvecklingen går emot starkare skydd för upphovsmän och att SVT inte kan hålla fast vid sin gamla praxis. Domstolen påpekade därtill att SVT var väldigt mån om att nämna sina egna medarbetare, fastän dessas roll kan vara av mindre betydelse. Möjligheterna att nämna namnen på kompositörerna när deras verk framfördes fanns alltid. Fråga var om att iaktta upphovsmännens behov av att bli nämnda och att utnyttjaren inte sätter egna intressen framom upphovsmännens.

Beslutet i detta fall uppfattades som en seger för de ideella rättigheterna eftersom risken alltid finns att dessa inte beaktas i den omfattning som god sed kräver i olika media. I detta fall gäller frågan att elektroniska media skall behandlas på samma sätt som traditionella media. Huvudprincipen är att upphovsmannens namn skall anges i enlighet med god sed när hans verk framställs och görs tillgängligt för allmänheten.

Namngivelse skall även ske vid offentliggörande i radio och TV, medan man i synnerhet i dessa medier kallar namngivelsen för kreditering. Denna kreditering anknyts enligt *Schönning* till upphovsmannens ekonomiska intressen inom ideella rättigheter. I och med att då upphovsmannen blir känd som skapare till sina verk, kan han få den renommé, som är betydelsefull för verkens marknadsföring och framtida arbetstillfällen. Krediteringen har också betydelse för identifieringen av rättsinnehavare i samband med de kollektiva ersättningarna. Intressant i sammanhanget är, att *Schönning* påpekar, att det inte spelar någon roll för namngivelseskyldigheten om den påför användaren utgifter.¹⁶

För upphovsmannen är det dels viktigt att av rent ideella personliga skäl bli omnämnd, men dels av ännu större vikt är den ovan nämnda ekonomiska aspekten. För upphovsmannen betyder det att hans namn blir mera känt, vilket sannolikt leder till att han blir mer efterfrågad av allmänheten. Frågan kan då gälla att användaren beaktar upphovsmannens intresse och behov att få erkänsla. Televisionen är ett av de bästa medierna för att öka attraktionen.

Det har saknats en ingrodd praxis eller sedvana på området när det gäller att namnge upphovsmannen i televisionsprogram. Beslutet att namnge upphovsmannen i samband med televisionsprogrammet är i enlighet med god sed enligt HD, trots att namngivningen inte hade stadgat sig på området i fråga eller varit en sedvana. Bestämmelsen om angivande av

¹⁶ Se SOU 1956: 25: 116 och sv.prop. 2004/05: 118 samt *Schönning* 1998: 166–167.

upphovsmannens namn gäller uteslutande när utnyttjandet av verket grundar sig på avtal med upphovsmannen.

Enligt god sed kan man inte försumma namngivelseskyldigheten, emedan man kan lämna uppgifterna om upphovsmannen på ett flertal olika sätt, exempelvis i tryckta program, muntligen i anslutning till programmet eller i en textremsa på bilden under sändningen. Att namnge upphovsmän i en samlad lista efter programmet då namnen bara rullas upp kan anses ”som en tom gest”.

Det kan dock förekomma situationer, där det är av mindre betydelse för upphovsmannen att hans namn anges, eller förhållanden där det är störande att ange namnet på upphovsmannen, såsom vid kyrkliga förrättningar, eller på restauranger, caféer har man ansett namngivelse vara utan betydelse. På restauranger och caféer är det här fråga om s.k. lugn bakgrundsmusik. Vid t.ex. liveframföranden skall nog namnet på upphovsmannen anges. I vissa fall kan det dock vara tekniskt svårt att ange namnet på upphovsmannen. Det kan understrykas att digital teknik ändå medger helt andra förutsättningar för namngivandet än analog teknik. Exempelvis innehåller ordbehandlingsprogram hypertextegenskaper som möjliggör att ta avsevärt mera information om upphovsmannen och källan i digitalt textmaterial.

Vid vissa tillfällen kan det dock uppfattas såsom störande och är följaktligen inte i enlighet med god sed, att ange upphovsmannens namn när hans verk görs tillgängligt eller framförs för allmänheten, såsom ovan nämnt då musikverk framförs t.ex. vid begravingar och dylika sammanhang, när musikverk används som bakgrundsmusik. Med en viss reservation kan påpekas, att man vid de flesta religiösa sammankomster får information om upphovsmännen i tryckta textblad eller psalmböcker. Gällande bakgrundsmusik vid restauranger går det att praktiskt ordna med angivande av upphovsmännen, eftersom man ofta har färdigt inspelade band på vilka man också kunde nämna upphovsmännen utan att gästerna blir störda. Namngivelse är också praktiskt möjlig på vissa typer av konstverk och design. I anslutning till utställningar är det angeläget att namnge upphovsmannen till den musik som framförs i samband med utställningen för att komplettera denna. Här är skyltning praktiskt och tekniskt möjlig.

I ett fall tog Svea Hovrätt, FT 3622–99, ”Museum” ställning till att upphovsmannen anges i den omfattning och på det sätt som god sed kräver. Hovrätten ansåg att det inte förelåg något praktiskt eller tekniskt hinder mot att ange upphovsmannen till musik, som framfördes i samband med en utställning, redan när utställningen öppnades. Hovrätten fann att museets underlåtenhet att namnge upphovsmannen under hela utställningstiden inte var förenlig med god sed.

Avsikten med kravet på god sed skall förstås såsom att 1) stöda en rådande praxis, ifall denna är en god sådan, 2) befrämja att en god praxis uppkommer ifall ingen sådan förekommer inom området ifråga. Den goda seden är lika angelägen såväl i analogt som digitalt sammanhang. Såsom Auktorrättskommittén insåg är situationen där att praxis inte ses som en norm, under alla omständigheter också sådana där lagregeln kan bli svår att tillämpa. Ifall lagstiftaren inte ställer upp klara regler för varje specifik situation, är det dock domstolarnas sak att tillsammans med experter inom området styra praxis så att en god sed utvecklas. I osäkra och oklara situationer kan det sålunda tolkas som bättre att upphovsmannens namn anges än motsatsen. Detta är inte endast i enlighet med upphovsmannens ideella intressen, utan har även en klar ekonomisk betydelse, emedan upphovsmannen kanske blir mer känd och kan skapa sig ett marknadsvärde. Lojalitetsprincipen framträder även i detta sammanhang, för upphovsmannen kan anse sig berättigad till att inte behöva erfara att utnyttjaren sätter sina egna intressen framom upphovsmannens, emedan den andra partens, såsom upphovsmannens, berättigade intressen (förmåner) bör beaktas i skäligen mån.

4.5. Databaser och datorprogram

Databaser och datorprogram är typer av litterära verk. Vad som är ett datorprogram definieras inte i upphovsrättslagen.

Endast fysiska personer kan ha ideella rättigheter till sina verk. En arbetsgivare eller juridiska personer, kan nog ha härledda ekonomiska rättigheter till verk som hans arbetstagare utfört i t.ex. tjänst eller under ledning av någon överordnad i hans företag.

Om rådande praxis angående paternitetsrätten, datorprogram och databaser, förekommer varierande uppfattningar om hur de skall tolkas. *Rosén* anser, att varje skapare av ett verk bereds tillfälle att kräva namnangivelse- och respekträtt. Enligt databasdirektivet tillkommer den ideella rätten av upphovsrätten till en databas upphovsmannen som skapat databasen och skall utövas i enlighet med medlemsländernas lagstiftning och enligt bestämmelserna i Bernkonventionen. Den ideella rättigheten faller utanför databasdirektivets tillämpningsområde. Upphovsmäns och andra rättsinnehavares intressen koncentreras på verk enligt 1 § URL och andra skyddsobjekt som eventuellt utgör innehåll i databaser enligt 49 § URL.¹⁷

I det förslag som kommissionen gav om databasdirektivet fanns ett stadgande om övergången av de ekonomiska rättigheterna till databaser skapade i arbetsförhållanden. Stadgandet avlägsnades dock från det slutliga direktivet och saken lämnades att avgöras av medlemsstaterna, såsom framkommer i direktivets ingressdel 29 punkten. I Finland löstes frågan genom att tillägga ett hänvisningsstadgande till 40b § 3 mom. URL, enligt vilket vad som bestäms om datorprogram tillämpas på motsvarande sätt på databaser vid utförande av arbetsuppgifter som följer av ett arbetsförhållande eller ett tjänsteförhållande. Upphovsrätten till databaser hör i alla situationer initialt till den fysiska person som är upphovsman till databasen. Enligt sagda hänvisningsstadgande övergår upphovsrätten till databasen till arbetsgivaren. Detta specialstadgande ansågs som ett undantag från upphovsrättens huvudregel, enligt vilken upphovsmannen har rätt att bestämma över sitt verk. Övergången av de ideella rättigheterna till databaser i arbetsförhållanden bands vid stadgandena om datorprogram. De ekonomiska rättigheterna till datorprogram och databaser, som skapas av en arbetstagare i en arbetssituation, övergår till arbetsgivaren, men för de ideella rättigheternas del är situationen annorlunda. Datorprogram- och databasdirektiven ger medlemsstaterna möjlighet att avgöra, huruvida också de ideella rättigheterna skall övergå till arbetsgivaren.

Upphovsrätten till ett verk hör enligt 1 § upphovsrättslagen ursprungligen till den som skapat verket. Föreskrifter angående övergången av rättigheten i ett arbetsförhållande ingår i finska 40 b § URL som innehåller ett specialstadgande angående övergången av upphovsrätten till datorprogrammet till arbetsgivaren. Övergången av upphovsrätten till datorprogram till arbetsgivaren vid utförande av arbetsuppgifter som följer av ett arbets- eller tjänsteförhållande innefattar endast de ekonomiska rättigheterna enligt 2 § URL. I förarbetena till lagen ansågs att på de ideella rättigheterna tillämpas vad som stadgas i 3 § URL. Samtidigt konstaterades att de nya bestämmelserna i 40 b § URL inte påverkade övergången av rättigheterna i arbets- och tjänsteförhållanden för andra verkskategorier än datorprogram. I 40a § svenska URL stadgas att upphovsrätten i sin helhet övergår till arbetsgivaren, ifall inte annat förutsätts av ett avtal.

Enligt de finska och norska upphovsrättslagarna kan inte de ideella rättigheterna överlåtas, medan de kan överlåtas enligt den danska lagen. Enligt norska NOU anser man uttryckligen att även programmeraren och andra som deltagit i utvecklingen av programmet skall namnges, om deras insats varit självständig och originell. Enligt *Schönning* gäller vid datorprogram, där en bred och

¹⁷ Se artikel 2(3) Datorprogram-direktivet 91/250/EG och ingresspunkt 28 Databas-direktivet 96/9/EG. Se dock *Rosén* 1995: 11, 13, 21–22 och *Välimäki* 2006: 33–34.

skiftande krets deltar i programutvecklingen, inte normalt en skyldighet att namnge upphovsmännen enligt dansk lag. Enligt *Koktvedgaard* kan man tala om en fullständig övergång, dvs. att också de ideella rättigheterna övergår. Han anser vidare, att varken paternitetsrätten eller respekträtten spelar någon större roll på detta område, men att det är av principiellt intresse, emedan man inte kan avtala om total övergång av de ideella rättigheterna. Dock hänvisas till datorprogramdirektivet, som endast omfattar de ekonomiska rättigheterna och att Danmark fritt kan reglera de ideella rättigheterna. De svenska lagstiftarna använde begreppet övergång istället för överlåtelse, vilket bl.a. *Rosén* ser som problematiskt, eftersom begreppet överlåtelse används för alla överlåtelser i URL som baserar sig på ett avtal. Att då använda begreppet övergång för samma sak ökar förvirringen. Därtill är vidareöverlåtelser av upphovsrättigheterna inte tillåtna enligt 28 § URL. När då begreppet övergång används istället för överlåtelse, kan det tolkas som om att det är tillåtet att de ideella rättigheterna övergår vidare, vilket säkert inte varit lagstiftarnas avsikt.

Upphovsrättsrådet i Finland var i ett fall 1998: 13 av den åsikten att principen om god sed i paternitetsrätten inte förutsätter att namnet på ett företag som tillverkar datorprogram avsedda för att skapa och visa informationsboxar behöver nämnas när dessa informationsboxar förevisas för allmänheten.

Enligt en rådande praxis inom branschen anges inte upphovsmannens namn p.g.a. att datorprogram eller databaser inte uppfattas på samma sätt som personliga verk skapade av upphovsmän. Man har inom branschen anammat ett ställningstagande att det inte förekommit en namnangivelseplikt eller sedvana. Detta kan delvis bero på att upphovsmännen till datorprogram och databaser antas ha mer ekonomiska intressen än ideella. Datorprogram eller databaser ses mera som produkter än som verk.

Dock kan man, som det påpekats, inte frånga kravet på att ange upphovsmannens namn i samband med datorprogram, annat än då det är praktiskt svårt eller omöjligt. Det kan vara fråga om dimensionsbrister eller att namnangivelsen påverkar utseendet, uppfattningen eller upplevelsen av verket. *Haarmann* påpekar att man inte kan avstå från namnangivelse enbart genom att hänvisa till god sed, man kan låta bli att nämna endast om detta förfarande är enligt god sed eller om man avtalat därom. Att underlåta att ange upphovsmannens namn är endast lovligt, om det är i överensstämmelse med en sedvana, som må betraktas som god, dvs. rimlig och hederlig, inte om denna sedvana inte är god. Även *Välimäki* förfäktar, att man inte alltid kan framskrida utan att namnge upphovsmannen, för många gånger hör namnangivelse av enskilda programmerare till sedvana och man är då skyldig att namnge upphovsmannen enligt lag.

I rättslitteraturen har ett allmänt uttryck blivit, att man i samband med datorprogram i allmänhet inte nämner originalupphovsmännen. Detta är möjligen en allmän sed, men det är en helt annan sak huruvida det är en god sed. Det förekommer inte något tekniskt hinder för att namnet på upphovsmännen till datorprogrammen nämns både i skilda skriftliga föreskrifter, ifall dylika förekommer, samt i själva programmen. Ett sådant förfarande vore enligt god sed, ifall saken granskas jämligt även med beaktande av upphovsmannens intressen. Det är enligt god sed att nämna upphovsmännens namn och inte lämna dem onämnda enligt den allmänt rådande kutymen.

Ifall upphovsmannens namn anges, kan detta ske i samband med programkoden vilket innebär att användaren till datorprogrammet blir medveten om upphovsmannens namn enbart i vissa särskilda situationer, till exempel då han förändrar koden för att göra en rättelse. Om användarna skall bli bättre medvetna om vem som är upphovsman till datorprogrammet de använder, kan upphovsmannens namn anges, till exempel på skärmen för första gången då programmet används eller varje gång programmet öppnas, vilket var vanligt förekommande på 1980-talet. Upphovsmannens namn kan även anges och framkomma i programmanualen. Huvudproblemet med att ange upphovsmannens namn är dock att programmanualerna inte nödvändigtvis följer med själva programmet.

Upphovsmännens namn behöver inte synas direkt på bildskärmen då programmet startas, utan kravet på god sed torde även uppfyllas, på så sätt att en förteckning över upphovsmännens namn blir synbar med ett särskilt kommando eller med hjälp av en skild aktiverande länk. Användaren kan därifrån få ifrågavarande uppgifter. Här är det inte frågan om att det skulle vara direkt tekniska, praktiska eller störande skäl som skulle hindra en namngivelse. Namngivelsen saknar inte betydelse, eftersom det kan vara ekonomiskt betydelsefullt för upphovsmannen att bli angiven som upphovsman, det är fråga om hans renommé och etablering på datorprogrammarknaden. Det kan vara fråga om att upphovsmannen önskar dra nytta av spridningen av sitt verk till den stora allmänheten och önskan om att hans verk skall skilja sig från andras verk. Information om upphovsmannen kan anses vara en skyldighet. Man kan tala om den goodwill som både företaget och upphovsmannen åtnjuter. För företaget innebär underlåtet att riskerna för att upphovsmannen kräver sin namngivelserätt överhängande enligt *Välimäki*.

Praxis att ange upphovsmannens namn i samband med datorprogram har dock även i Finland uppfattats som begränsad. Där behov framkallats har man följaktligen tagit stöd av motiveringarna i regeringens proposition, där det ansågs, att man på de ideella rättigheterna tillämpas vad som stadgas i 3 § URL. Hänvisningar har gjorts till att det enligt i branschen rådande god sed i allmänhet inte förutsätts att upphovsmannens namn nämns. Man har ansett att eftersom programmets natur och användning i väsentlig grad avviker från andra slag av verk, har dessa rättigheter när det gäller datorprogram en liten betydelse. Motiveringar för att följa en god sed i branschen har framförts ovan.

Delvis omfattas denna praxis i stort av upphovsmännen ifråga och verkar också vara den rådande internationellt, främst på grund av inflytande från USA, där det kommersiella måhända är starkare än det ideella. *Wilhelmsson* anser att näringslivets egna principalsamlingar och allmän praxis i branschen inte kan användas som något betydande argument för ett förfarandes lagenlighet¹⁸. Till exempel i fall en bred och skiftande krets av upphovsmän deltar i programutvecklingen, har man i Danmark ansett att det inte finns något krav på att ange upphovsmännens namn. Ifall dock upphovsmännen ifråga insåg att namngivelsen kunde inbringa ekonomisk vinning, kunde de börja kräva att deras namn framkom i samband med de datorprogram de skapat.

4.6. Bearbetningar

Paternitetsrätten omfattar också bearbetningar. Enligt 4 §, nordiska upphovsrättslagarna har den som översatt eller bearbetat ett verk eller överfört det till en annan litteratur- eller konststart upphovsrätt till verket i den gestalten, men han får inte förfoga över verket på ett sätt som står i strid mot upphovsrätten till originalverket. Bearbetningar till litterära verk är bland annat sammanfattningar och kompletteringar av dem. Den vanligaste bearbetningen av musikaliska verk är arrangemang av det. Till bearbetningar hör också ett fotografi av en tavla och en målning av ett fotografiverk samt uppdatering av ett datorprogram och utveckling av det genom att t.ex. tillägga nya funktioner. En bearbetning förutsätter någonslags omarbetning av verket i något avseende, såsom tillägg, borttagning av delar av verket eller stilmässiga förändringar. Ändringar av mindre slag, såsom rättande av fel, är inte bearbetningar. Det samma gäller mekaniska funktioner, såsom översättning av en enkel och kort manual (till exempel en mekanisk översättning från ord till ord) och en översättning av ett datorprogram från ett datorspråk till ett annat, ifall det bara är en teknisk åtgärd. Ifall någon i fri anslutning till ett verk skapat ett nytt och självständigt verk, är dennes upphovsrätt inte beroende av upphovsrätten till originalverket. När en bearbetning är gjord enligt 4 § 1 mom. URL, skall namnen på upphovsmännen anges enligt 3 § 1 mom. URL.

¹⁸ Se *Wilhelmsson* 1989: 125.

Till exempel kan upphovsmannen till en översättning av ett litterärt verk till ett annat språk eller en revidering av ett verk från en konstart till en annan erhålla upphovsrätt till bearbetningen. Rätten till den bearbetade versionen omfattar endast den versionen. För att få utnyttja den bearbetade versionen krävs medgivande av både den ursprungliga upphovsmannen och bearbetaren. Bearbetningen bör nå den s.k. verkshöjden för att omfattas av upphovsrätten, dvs. uppvisa tillräcklig originalitet och vara ett resultat av upphovsmannens självständiga skapande verksamhet. När bearbetningar görs tillgängliga för allmänheten och exemplar framställs av dem, är det i enlighet med principen om god sed att namnet på både upphovsmannen till originalverket och bearbetaren anges. Det innebär att avstegen i form av svårigheten att namnge, såsom ovan beskrivits, omfattas även av bearbetningar. Exempelvis kan svårigheter inte rimligtvis föreligga vid översättningar. Lagregeln kan belysas med det att, för att få översätta ett verk krävs medgivande av upphovsmannen, ifall man ämnar använda verket för annat ändamål än för eget bruk i enlighet med 12 § URL. Till exempel om det är fråga om en engelsk text som skall översättas till svenska, krävs medgivande av upphovsmannen till den engelska texten då översättningen görs tillgänglig för allmänheten. Översättaren får upphovsrätt till den översättning av verket som han gjort. I enlighet med principen om god sed är det då naturligt att namnet på både översättaren och upphovsmannen till originalverket anges.

När det uttryckligen är fråga om flera upphovsmän är det i enlighet med god sed att åtminstone ange namnen på de upphovsmän vars insats eller bidrag i skapandet av verket är så originellt och självständigt att det uppnår verkshöjden:

Ett rättsfall i Vasa hovrätt 27.12.1985 handlade det om en katalog över postkort. Frågan som skulle avgöras var huruvida förutom B också A hade upphovsrätt till katalogen. Avgörande var inte hur mycket eller på vilket sätt A hade bidragit till samlingen av postkorten eller till klargörandet av informationen om postkorten. Däremot var det avgörande huruvida A hade bidragit med idéer hur katalogen över postkorten skulle skapas och formas.

I fallet framkommer att det i enlighet med principen om god sed kan uppfattas som självklart att en upphovsman inte skall få erkänsla på andra upphovsmäns bekostnad för ett verk han inte deltagit i eller bidragit till. Det är, å andra sidan, ytterst viktigt att de upphovsmän, vars bidrag varit tillräckligt självständiga och originella, anges i samband med verket då detta påverkar deras legitima status som upphovsmän.

Kravet på god sed inom paternitetsrätten gäller följaktligen alla typer av upphovsrättsskyddade verk och den praxis som gäller inom varje specifikt område kan tillämpas även inom respektive område i den digitala miljön. Faktum är att digitala teknologiska lösningar inte bara utgör ett hot mot skyddet av upphovsrättigheterna utan kan erbjuda ytterligare bättre och mera omedelbara möjligheter till skydd.¹⁹

5. Summary

The legal principle of fair practice has its origin in Roman law, where there existed a legal rule whereby a debenture that did not accord with fair practice (contra bonos mores) was considered invalid. The principle of fair practice can be seen as both a moral and a legal norm. The duty to obey a moral norm can have its basis in a common conception in society as to what is proper or valued behavior. The duty to obey a legal norm has its basis in a command by the legal system to act according to the law.

¹⁹ Se Koivumaa 2004: 32.

The paternity right implies that the name of the author should be stated when one of his or her works is made available to the public and especially when it is performed publicly in a manner required by fair practice. What is deemed fair practice varies according to different categories of works and according to the circumstances of a particular case; accordingly, it is case law that has had to decide what is to be conceived as fair practice in the case of the paternity right.

In the visual arts the basic rule is that the name of the author is to be stated in all cases when it is not disruptive and when technical or practical reasons do not require otherwise. In the case of literary works it is of no relevance for the paternity right to what extent a copyright protected work is used, as long as it can be identified as created by a specific author. It is also of no importance whether the work is made available to the public in an arranged form, with a new technique or in a new medium as long as the author of the work can be connected to the work. In musical works it has not been considered permissible to remove the name of the author from works that are made available to and performed to the public; for example, the principle of fair practice implies that the name of the author and the performing artist are to be stated when their musical works are performed in both analog and digital media. In the case of databases and computer programs, there is a rule whereby the name of the author is not stated where the works in question are not viewed as personal works created by the authors; however, it has been pointed out that the duty to state the name of the author is not to be sidestepped where it is not practically difficult or completely impossible to mention it. Where works created by many authors are involved, it is in keeping with fair practice to at least state the names of the authors whose effort or contribution to the creation of the work is so original and independent that it attains the level required for a copyrightable work.

The requirement of fair practice in the case of the paternity right applies to all types of copyright-protected works and the case law in the different areas of copyright can be applied to analogous cases in the digital environment.

6. References

Aarnio, Aulis (1989). *Laintulkinnan teoria*. Juva: WSOY.

Bernitz, Ulf, Gunnar Karnell, Lars Pehrson & Claes Sandgren (2009). *Immaterialrätt och otillbörlig konkurrens*. Elfte upplagan. Stockholm: Handelsbolaget Immateriellt Rättsskydd.

Betaenkning 1064/1986. Ophavsret og edb. København.

Betaenkning 1197/1990. Revision af ophavsretslovgivningen. Slutbetaenkning fra Udvalget vedrørende revision af ophavsretslovgivningen. København.

Bruun, Niklas (2001). *Intellectual Property Law in Finland*. Helsinki: Kauppakaari Oyj.

Europeiska Gemenskapernas Direktiv (1991). Rådets Direktiv om rättsligt skydd för datorprogram (91/250/EEG).

Europeiska Gemenskapernas Direktiv (1996). Rådets Direktiv om upphovsrättsligt skydd för databaser (96/9/EEG).

Forslag til lov om ændring af ophavsretsloven L17, L19, November 2002. København. Danmark.

Haarmann, Pirkko-Liisa (2005). *Tekijänoikeus ja lähioikeudet*. Helsinki: Talentum Media Oy.

Herler, Brita Kristina (2011). *Upphovsrätt, särskilt vid universitet och högskolor*. 5 rev.uppl. Vasa: Brita Herler.

Karhu, Juha (2005). Tekijänoikeus. In: *Oikeusjärjestys 2000 osa III*, 3. täydennetty painos, 271–306. Toim. Risto Haavisto. Lapin yliopiston oikeustieteellisiä julkaisuja, sarja C 38. Rovaniemi: Lapin yliopiston oikeustieteiden tiedekunta.

Karhu, Juha (2006). Tekijänoikeus. In: Oikeusjärjestys 2000 osa III, 4. täydennetty painos, 279–316. Toim. Risto Haavisto. Lapin yliopiston oikeustieteellisiä julkaisuja, sarja C 43. Rovaniemi: Lapin yliopiston oikeustieteiden tiedekunta.

Kivimäki, T.M. (1966). Uudet tekijänoikeus- ja valokuvalait. Porvoo: WSOY.

Koivumaa, Ari (2004). Johdatus tekijänoikeuden perusteisiin erityisesti informaatioteknologian näkökulmasta. [online]

Komiteanmietintö-Kommittébetänkande 1987: 8. Tietotekniikka ja tekijänoikeus. Teosten luominen ja käyttö tietokoneen avulla tietokoneohjelmien, tiedostojen ja tietokantojen sekä integroitujen piirien suoja. Tekijänoikeuskomitean IV osamietintö. Helsinki: Opetusministeriö.

Komiteanmietintö-Kommittébetänkande 1990: 20. Oikeustoimilakitoimikunnan mietintö. Helsinki: Opetusministeriö.

Komiteanmietintö-Kommittébetänkande 2002: 5. Tekijänoikeustoimikunnan mietintö. Tekijänoikeudet tietoyhteiskunnassa. Helsinki: Opetusministeriö.

Komiteanmietintö-Kommittébetänkande 2012: 2. Upphovsrättskommissionens betänkande: Lösningar till digitala tidens utmaningar. Helsingfors: Undervisnings- och kulturministeriet.

Koktvedgaard, Mogens & Marianne Levin (2003). Lärobok i immaterialrätt. Stockholm: Norstedts Juridik AB.

Levin, Marianne (2011). Lärobok i immaterialrätt. Stockholm: Norstedts Juridik AB.

Mähönen, J. (1995). Law and economics: Taustaa ja mahdollisuuksia. Oikeus 2, 125–139.

Niemi, Markku I. (1998). Holismi ja konventionalismi. Lainopit keskeiset episteemiset käsitykset. Lakimies 4/1998, 521–538.

Norges offentlige utredninger. NOU 1986: 18. Ophavsret og EDB. Oslo: Universitetsforlaget.

Nuotio, Kimmo (2004). Oikeuslähteet ja yleiset opit. Lakimies, 7–8/2004, 1267–1291.

Odelstingsproposisjonen 26 (1959–60). Oslo: Kirke- og undervisningsdepartementet.

Peczenik, Alexander (1988). Rätten och förnuftet. Stockholm: Norstedts.

Pohjonen, Marja (1993). Hyvä tapa ja oikeuskäytäntö eräillä immateriaaioikeuden aloilla. In: Hyvän tavan vastaisuudesta, 137–172. Toim. Ari Saarnilehto. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. No. 2. Turku: Turun yliopisto

Pöyhönen, Juha (1999). Hyvä tapa. In: Encyclopedia iuridica fennica. VII Oikeuden yleistieteet, 197–199. Toim. Heikki Mattila. Suomalaisen Lakimiesyhdistyksen julkaisuja C-sarja n:o 30. Helsinki: Suomalainen lakimiesyhdistys.

Rosén, Jan (1989). Förlagsrätt. Rättsfrågor vid förlagsavtal. Stockholm: Juridiska fakulteten i Stockholm, skriftserien 23. Stockholm: Juristförlaget.

Rosén, Jan (1995). Swedish Software Law. Stockholm: Juristförlaget JF AB.

Rosén, Jan (1996/97). Ideell rätt i praktiken. JT, 142–147.

RP 161/1990 rd. Regeringens proposition till riksdagen med förslag till lag om ensamrätt till kretsmönster för integrerade kretsar samt till lagar om ändring av upphovsrättslagen, lagen om rätt till fotografisk bild samt lagen om patent- och registerstyrelsen. Helsingfors: Statens Tryckericentral.

RP 211/1992 rd. Regeringens proposition till riksdagen med förslag till lag om ändring av upphovsrättslagen och av 2 mom. i kraftträdelsestadgandet i lagen om ändring av upphovsrättslagen. Helsingfors: Statens Tryckericentral.

RP 287/1994 rd. Regeringens proposition till riksdagen med förslag till lag om ändring av upphovsrättslagen och lag om upphävande av lagen om rätt till fotografisk bild. Helsingfors: Statens Tryckericentral.

RP 170/1997 rd. Regeringens proposition till riksdagen med förslag till lag om ändring av upphovsrättslagen och med förslag till lag om ändring av 49 kap. 1 § strafflagen. Helsingfors. [online, available at: <http://www.eduskunta.fi>]

RP 28/2004 rd. Regeringens proposition till riksdagen med förslag till lagar om ändring av upphovsrättslagen och 49 kap. strafflagen. Helsingfors. [online, available at: <http://www.eduskunta.fi>]

Saarnilehto, Ari (1992). Hyvää tapaa koskevista säännöksistä. In: Hyvä tapa, 5–16. Toim. Seija Huhtamäki. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. C: 16. Turku: Turun yliopisto.

Saarnilehto, Ari (1993). Alkusanat. In: Hyvän tavan vastaisuudesta, 1–15. Toim. A. Saarnilehto. Turun yliopiston oikeustieteellisen tiedekunnan julkaisuja. B No 2. Turku: Turun Yliopisto.

Saarnilehto, Ari (2005). Sopimusoikeuden perusteet. Helsinki: Talentum.

Schønning, Peter (1998). Ophavsretsloven med kommentarer. 2. udgave. København: Gadjura.

Sorvari, Katariina (2005). Vastuu tekijänoikeuden loukkauksesta. Erityisesti tietoverkkoympäristössä. Yliopistollinen väitöskirja. Helsinki: WSOY.

Sorvari, Katariina (2007). Tekijänoikeuden loukkaus. Helsinki: WSOYpro.

SOU 1956:25. Statens offentliga utredningar. Upphovsmannarätt till litterära och konstnärliga verk. Lagförslag av auktorrättskommittén. Stockholm: Justitiedepartementet.

Strömholm, Stig (1966). Le droit moral de l'auteur en droit Allemand, Français et Scandinave avec un aperçu de l'évolution internationale II:1 Deuxième partie. Stockholm: Norstedt & Söners Förlag.

Strömholm, Stig (2002). Droit Moral - The International Comparative Scene from a Scandinavian Viewpoint. In: Scandinavian Studies in Law Volume 42, 217–253. Stockholm: The Stockholm University Law Faculty.

Sv. prop. 1988/89: 85. Svenska regeringens propositioner. Upphovsrätt och datorer. Stockholm.

Sv. prop. 2004/05:110. Svenska regeringens propositioner. Stockholm.

Tolonen, Hannu (2003). Oikeuslähdeoppi. Helsinki: Werner Söderström Lakitieto Oy.

Udkast til lov om ophavsretten (1951). København.

Välimäki, Mikko (2006). Oikeudet tietokoneohjelmistoihin ja niiden lisensiointi. Helsinki: Turre legal.

Watson, A. (1984). An approach to customary law. University of Illinois Law Review.

Wilhelmsson, Thomas (1989). Konsumentskyddet i Finland. Helsingfors: Juristförbundets Förlag.

von Wright, Georg Henrik (1963). Norm and Action. A logical enquiry. London: Routledge & Kegan Paul.

Ämmälä, Tuula (2001). Hyvän tavan vastaisuus. In: Varallisuus oikeus, 123–129. Toim. Ari Saarnilehto, Mika Hemmo & Leena Kartio. Helsinki: WSOY.

A RIGHT TO KNOWLEDGE AND INFORMATION – AND SUBJECTIVE RIGHTS

Wolfgang Mincke

Professor Dr. Dr.h.c Rechtsanwalt, University of Lapland, Finland
Schleiermacherstrasse 23, 30625 Hannover DE
wmincke@web.de

Keywords: *Right to knowledge, subjective rights, specificity, publicity, scarcity, patent, copy-right*

Abstract: *It seems that in a legal world that is governed mainly by economic argumentation if not dictated by business interests the criteria and tools offered by jurisprudence have been on a retreat. It is an essential task for jurisprudence to avert the institution of subjective rights that may stand in the way of free access to knowledge and information for everybody. Before creating new branches of jurisprudence to deal with allegedly novel problems a return to traditional legal science with its presumably globally valid principles might give a valuable guidance.*

1. A subjective right to information?

1.1. The legal basis

At first glance one might ask whether and where there is a problem. The right to have access to knowledge and information as a right of everybody seems as a matter of course. It is expected to be an integral part of any democratic state and so it is found in the constitutions of most states.

The German constitution: Art 5 GG, Freedom of expression, arts and sciences:

“(1) Every person shall have the right freely to express and disseminate his opinions in speech, writing and pictures, and to inform himself without hindrance from generally accessible sources. ...”

This seems clear enough. The article explicitly mentions a right of everyone to information. All modern constitutions - of enlightened states at least -, contain an accordant clause.¹ Isn't this enough as an argument that a right to knowledge is apparently well established and generally accepted?

One first thing should make us hesitate: The articles of the constitution regulate the relation between the state and its citizens. They grant freedom against interference by the state and its authorities. This is how the right of citizens to information and thus to knowledge predominantly has been dealt with. What has been and is discussed in the European Union has an even narrower scope: The central theme has been access to information held by the state and its authorities, so-called “public sector information”, or short: PSI.

¹ Finnish constitution: Section 12 - Freedom of expression and right of access to information: “Everyone has the freedom of expression. Freedom of expression entails the right to express, disseminate and receive information, opinions and other communications without prior prevention by anyone.”

„Public sector information (PSI) is the single largest source of information in Europe. It is produced and collected by public bodies and includes digital maps, meteorological, legal, traffic, financial, economic and other data. Most of this raw data could be re-used or integrated into new products and services, which we use on a daily basis, such as car navigation systems, weather forecasts, financial and insurance services.

Re-use of public sector information means using it in new ways by adding value to it, combining information from different sources, making mash-ups and new applications, both for commercial and non-commercial purposes. Public sector information has great economic potential. According to a survey on existing findings on the economic impact of public sector information conducted by the European Commission in 2011 (Vickery study) the overall direct and indirect economic gains are estimated at €140bn throughout the EU. Increase in the re-use of PSI generates new businesses and jobs and provides consumers with more choice and more value for money.“²

This statement is in line with Directive 98/2003 EG on the re-use of information. This Directive establishes a minimum set of rules governing the re-use and the practical means of facilitating re-use of existing documents held by public sector bodies of the Member States.

In Germany this directive has been implemented by a Law on Freedom of Information of 2005 (Informationsfreiheitsgesetz)³ and the Law on Re-use of Information of 2006 (Informationsweiterverwendungsgesetz)⁴. Both deal exclusively with rights to be used against the state to access information held by the state and its authorities. This is clearly expressed in the complete title of the “Informationsfreiheitsgesetz” which is: Law Regulating the Access to Information Held by the Federation (Gesetz zur Regelung des Zugangs zu Informationen des Bundes). The same holds for the “Informationsweiterverwendungsgesetz” where the complete title is: Law on Re-use of Information Held by Public Authorities (Gesetz über die Weiterverwendung von Informationen öffentlicher Stellen (Informationsweiterverwendungsgesetz).

Apparently this European and national legislation does not care so much about freedom of knowledge and a right to knowledge as a personal right; it cares about economic welfare, rather. In the Law on Freedom of Information a right to information is not mentioned at all; it speaks about a claim (Anspruch) to access public sector information. The Law on Re-use of Information regularizes how to apply for re-use of information and guarantees equality of applicants, it does not grant a claim itself for access to or re-use of information.⁵

A broader scope seems to be represented in art. 10 of the European Convention on Human Rights:

Freedom of expression

1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for pre-

² “Raw Data for New Services and Products”, http://ec.europa.eu/information_society/policy/psi/index_en.htm.

³ Informationsfreiheitsgesetz vom 5. September 2005 (BGBl. I S. 2722).

⁴ Informationsweiterverwendungsgesetz vom 13. Dezember 2006 (BGBl. I S. 2913)

⁵ So Directive 98/2003 on the re-use of public sector information in recital 9: “This Directive shall not contain an obligation to allow re-use of documents. ... The Directive builds on the existing access regimes in the Member States and does not change the national rules for access to documents.”

venting the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

This article seems to reflect the struggle for knowledge that has given an undertone in history since earliest time, mainly against suppression of knowledge. Knowledge, whatever its quality, in many cultures has often been held secret, as an arcanum, accessible for privileged and initiated adepts only. A long way had to be taken that led from the institution of universities in the middle ages through renaissance and enlightenment to the introduction of compulsory school attendance, thus opening the way to acquire knowledge autonomously. Modern states seem to have taken their task seriously offering amongst others public radio and television channels for the promotion of knowledge for the general public.

1.2. Different concepts behind the word “right”

Modern legislation seems to point in the direction at least of a right to information and knowledge. Do they offer the subjective right to knowledge we are looking for? Some remarks have to be made concerning the word right. The word “right” is ambiguous. This ambiguity seems often to be neglected.⁶

Three instances, where the word is used in a different meaning, might serve as a help for explanation:

1. Somebody has the right to demand payment from a debtor.
2. Somebody has a right to an object, a car or a piece of land.
3. Everybody has the right to roam freely and undisturbed on unfenced ground.

There seems to be a common core for all these instances of the use of the word right. In all instances is spoken about a certain power the holder has. This has been and is often seen as the constitutive element of the concept of rights. Whether this holds true or not, shall not be the question here. But, that different concepts have a common core is no reason to abstain from further differentiation between them.

For the use of the word right in the first case most or many national legal orders have an own term: *claim*, *Anspruch* (German), *réclamation* (French), *(rechts-)vordering* (Dutch), *vaade* (Finnish).⁷ When the word right is used with the meaning claim, it refers to the relation between a creditor and a debtor. For those who prefer formalism: Right in the sense of claim is a predicate, which must have at least two arguments, both representing persons, to produce a complete proposition: $P(x,y)$ meaning “x has a claim against y”.

In the second case the word „right“ is used to express the rightholder’s legal position in respect to an object, a good. Somebody is owner of a car, holder of a patent or of a copyright or he is a creditor who has a receivable in his property. Here the word „right“ indicates that an asset is a piece of property, an item of a person’s legal estate, something that is his, exclusively, and that he can dispose of. In this sense Roman jurists spoke about a *ius in re*⁸. In this sense a right has and must have an object: land, chattel, a technical invention, a product of creative labour⁹. Formally: This right as a predicate needs only one argument, the holder of that right, to make a complete proposition: $P(x)$

⁶ The following differentiation is a sketch only, leaving much room for discussion

⁷ Roman law did not use a special word for this relation; it was concentrated on the procedural aspect of enforcement with the central concept of “actio”; this aspect still prevails in the jurisprudence of different countries

⁸ English legal terminology speaks about *ius in rem*, which blurs the difference between property ownership and claim.

⁹ It is not so apparent what this object is in case of a receivable; without delving deeper into this question: It is apparent that the receivable is a piece of property and a creditor can dispose of his receivable in the very same way as the owner of a car.

meaning “x owns the car”. It is this use of the word right that stands for the concept of subjective rights.

The third case seems special. Such rights have no specific “debtor”, and it is difficult to determine an object for them. They might be seen as part of the fundamental rights (civil liberties, civil rights), warranted in the constitution of most countries and in the European Convention of Human Rights. Such rights seem not to provide a certain object to the citizens but, rather, to ensure that vital activities can be performed without interference of the state and its authorities. So they are special in that they are not directed against fellow citizens but against public authority. In a well ordered state the state will procure that privates, too, will not interfere with the liberties of their fellow citizens. But the constitutionally guaranteed fundamental rights cannot be invoked directly against interference by fellow citizens.¹⁰

Among these three uses of the word “right” only the second meets the meaning of “subjective right”. In this sense a right legally allots an object to its owner as his property. This right is assured by claims (or actions) at the disposition of the owner. Such claims vary in different legal orders, in Common Law we know these as claim against trespass, unlawful withholding, action of trover and others. In Civil Law countries the most important claims of the owner are based on the vindictio and the actio negatoria of Roman Law. Property ownership as a subjective right is closely connected to the claims. Claims serve to realize the subjective right and to defend it (therefore they have been suitably named “secondary subjective rights”).¹¹

1.3. Which concept fits the right to knowledge?

The examination whether a right to knowledge would qualify as a subjective right has to decide in which of these three categories of rights the right to knowledge has to be seen. It does not seem sensible to understand the right to knowledge generally as a claim. In a political sense one might imagine that a right of the citizens to knowledge is claimed, when in a town-council a new library or a new school is discussed. But this is not the kind of claim that can be realized with the help of courts.

There are instances, where a person can claim to be informed and violation of this right will have consequences for the obliged partner: When selling an appliance the seller is obliged to inform the buyer about possible dangers from the use of that appliance. When shares of a company are sold by public offer, the state of the company has to be disclosed in all relevant details in a prospect. The same applies when capital is invested in a fund: The fund manager will be responsible to report about possible risks of the investment. Or, if you simply make a reservation for a holiday resort, you have a right to be informed correctly about the relevant properties of that resort. These all are special situations, where the right to information and the corresponding duty to inform arise as a corollary in a specific transaction. This information completes the representation of the asset that is to be purchased.

Also the case of the right to access to public sector information can best be understood as a claim. The German Law on Freedom of Information (Informationsfreiheitsgesetz) speaks explicitly of a claim for access to official information (Anspruch auf Zugang zu amtlichen Informationen) in its very first sentence. The directive on re-use of public sector information however states in the Recital (9): “This Directive does not contain an obligation to allow re-use of documents. The decision whether or not to authorise re-use will remain with the Member States or the public sector body

¹⁰ In this sense the law of most northern countries offers something special, so-called everyman’s rights which can be invoked against everybody (jokamiehen oikeudet in Finnish, in Swedish allemansrätt). They warrant the right to roam in the country where this does not disturb or harm the landowner, including the right to set up a tent, to pick berries and other activities. The Swedish constitution mentions the allemansrätt in § 2 kap. 15.

¹¹ „sekundäre Rechte“, so Raiser, Der Stand der Lehre vom subjektiven Recht im deutschen Zivilrecht, Juristenzeitung 1961, p. 465 ss.

concerned.” The German implementation of the directive then states in § 3 (1) of the Informationsweiterwendungsgesetz accordingly: A claim for access to information cannot be based on this law¹². It is the Law on Freedom of Information which complements the implementation of the directive granting the claim for access.

But the claim for access to public sector information again is a special case of a right to information. The function of the public sector is public, it is controlled by public authority, and financed by taxes levied from the general public. So it is only consequent that the informational products of the public sector are public and accessible by their own nature with the exception, of course, of data which have to be concealed because of their personal character or because of national security concerns etc. Rules for access to public sector information are not needed, to make this information public, but rather to forestall suppression of information and to regulate the procedure of giving access to such information.

The claim for access to public sector information cannot be expanded by any analogy into a general claim for access to information and knowledge. Accordingly there exists no general duty to disclose information or knowledge (with exceptions, such as witnesses who have to appear in court to report what they know about a certain incident).

The absence of a general claim for access to knowledge and information already precludes the existence of a subjective right to information and knowledge. Information and knowledge is no suitable candidate for property. Information is never owned in a sense that it is exclusively somebody's; somebody might conceal “his” information, but this does not hinder others to acquire the same information. In a sense, of course, somebody can dispose of information by revealing it to others, but that is of no influence on his information, it does not diminish his own knowledge.

After it does not seem sensible to see the right to knowledge and information as a claim or as a subjective right, there remains the possibility to understand the right to information and knowledge as a right in that sense that above has been typified as the third case: a right with no object and no debtor, as an everyman's right, as the natural right of a free man using his senses.¹³ It is one of the main characteristics totalitarian systems are built on that they have to bar the access to information other than such checked for conformity with official doctrine and ideology.

1.4. The Task of Legislation

Indeed, information has an especially important role in democratic societies that goes far beyond the economic value stressed by EU authorities¹⁴. To be informed is the first and indispensable condition for every rational decision. It does not need argumentation that better information makes better decisions. It therefore is a command of equality that all citizens have equal access to all available information. It is no serious counterargument that an excess of information can be an obstacle for rational decision. An inequality, no legislation can overcome, is the inequality of competence to deal with information. But it is an important aspect of the progress of IT that it offers more and better tools to find one's way through thickets of information.

This gives reason to turn the view around: Above it has been stated that in a well ordered state it will be procured by legislation that the liberties of citizens are respected. And this should involve that legislation secures access to all kinds of information¹⁵. It is understood that a democratic mind-

¹² „Ein Anspruch auf Zugang zu Informationen wird durch dieses Gesetz nicht begründet.”

¹³ This type of right might be seen as the deontic modality of permittedness allowing by negations the derivation of obligation and prohibition.

¹⁴ S. above, footnote 1; cf. the so-called “Vickery study under:

http://ec.europa.eu/information_society/policy/psi/docs/pdfs/report/psi_final_version_formatted.docx.

¹⁵ Cf. von Lewinski, Recht auf Internet, in: Rechtswissenschaft 2011, p. 70 ff.

ed state itself will not directly interfere with freedom of information of its citizens, but take measures only if such is demanded by moral, national concerns, security or other conditions as stated in art. 10 para. 2 of the European Convention on Human Rights. But there is an indirect way how access to information and its use can be barred by the state and its legislation. The state could give exclusive rights to single persons granting them a subjective right to a “piece” or a certain kind of information.

Apparently this possibility has been seen by the directive on re-use of public sector information¹⁶. In art. 11 para. 1, 2nd sentence it explicitly provides that contracts or other arrangements shall not grant exclusive rights. In para. 2, though, it allows that exclusive rights are granted “for the provision of services in the public interest”¹⁷. Furthermore, it explicitly leaves untouched national provisions which put the use of information under a license or some other kind of authorization.¹⁸ The directive gives evidence that its motivation is not so much the idea of free access for and freedom of information as a general aim, but the directive is motivated by the economic advantage it expects from free access to information, rather.

The conclusion must be here that access to information is access to reality. In an enlightened pluralistic democratic society no obstacle induced by law may bar access to reality.

2. Right to information as absence of restraining subjective rights

2.1. The right to information and intellectual property rights

Though freedom of information is a constitutional right, intrusions into this freedom by exclusive rights would be expected mainly in the field of private law. This gives cause to explore what the chances of such exclusive rights are, when the standards of general private law are applied.

Main candidates for exploration are the so-called rights of intellectual property. Here the word “intellectual” points into the direction of the intelligible world, thus to reality. “Intellectual” then should be understood as the rational rendition of something mental including information about the real world. “Property” on the other side points into the direction of a right that awards exclusivity. So the term intellectual property would include an exclusive, subjective right to the rational rendition of something real that thereby is reserved for the enjoyment and exploitation of a private right-holder. This contradicts evidently the principle that access to information about the real world must be free for everybody as a precondition and command of equality. The term “intellectual property” seems to be self-contradictory, to exhibit a *contradictio in adiecto*.

Whatever the merits of legal logic, contradictions - in this case a semantic contradiction – should have no place in any rational argumentation. If a contradiction is not seen as a stop-sign, at least it should be taken as a serious warning: We are leaving secure ground! For intellectual property this means: If we have good reason to protect intellectual products by subjective rights, then we should be extremely conscious of what we do and keep the inroad in strict limits. This is a challenge for traditional jurisprudence and a request to inspect its tools for guidance to maintain its rationality.

¹⁶ See above, footnote 4.

¹⁷ Cf. Recital (20): “However, in order to provide a service of general economic interest, an exclusive right to re-use specific public sector documents may sometimes be necessary. This may be the case if no commercial publisher would publish the information without such an exclusive right.” and Article 11 “Prohibition of exclusive arrangements”: 1. The re-use of documents shall be open to all potential actors in the market, even if one or more market players already exploit added-value products based on these documents. Contracts or other arrangements between the public sector bodies holding the documents and third parties shall not grant exclusive rights. 2. However, where an exclusive right is necessary for the provision of a service in the public interest, the validity of the reason for granting such an exclusive right shall be subject to regular review”.

¹⁸ Cf. Recital (9) and (17).

2.2. General principles of private law and intellectual property

Legal science has developed through centuries a canon of principles which govern subjective rights. Subjective rights in an object demand that certain criteria are fulfilled: specificity, publicity, exclusivity, fungibility; the number of subjective rights is limited (*numerus clausus*), private parties cannot create new subjective rights by any legal act¹⁹ – only legislation can create new subjective rights. These principles can be said to have a global validity, though such principles nowadays usually evoke the suspicion of outmoded dogmatism, far from the flexibility demanded by modern life. In place of delving into clarification of the merits of such principles with pertinent endeavour, here some short remarks to argue the plausibility of their benefit must suffice.

a) Specificity

Often scolded legal dogmatics can be seen (or have to be seen) as an essential component of our personal freedom, escorting the liberty rights granted by constitutions. The significance of specificity, the principle that subjective rights can only exist in individual objects, goes far beyond the examples we use in academic schooling: the fate of motors being fixed in car bodies, mixed trading stocks, or the fate of a central heating being installed in a house, where the oven looses or does not lose its legal individuality because it has become part of the house. Specificity has the meaning as well that a whole category or kind of things cannot be the object of a subjective right. We know this from the acquisition of an enterprise not by share deal but by asset deal: In this case the estate of a company cannot be acquired as a whole but must be transferred item by item. The property of a company itself is no valid subject matter in law which as such can be owned or transferred. Ownership refers only to the single individual objects the property is composed of.

Specificity can even be seen at the root of anti-monopoly and competition legislation. Law reacts to the pure fact already that one or few producers or traders can get hold of and dispose of a certain product or kind of products. By anti-monopoly legislation access to this kind of products is kept open for everybody who intends to compete as a part of personal and professional freedom (with the positive side-effect of keeping prices adequate).

b) Publicity

Similar considerations apply with regard to publicity as a general principle governing subjective rights. Publicity relates to the existence of the right and its right-holder and to any transactions concerning these rights. Prominent examples for the publicity of rights are public registers, where rights and transactions are documented and thereby communicated to the public. Publicity does not mean that always a broad public is addressed; more often it is only the concerned parties who are the addressees of the information about a right and its possible changes. Prominent example of publicity in many legal orders is that in transfer of property to chattels handing over of the item in question (the *traditio* of Roman law) is demanded. Correspondingly, when a receivable is transferred, a notice to the debtor secures publicity.

Arguably the principle of publicity has not been followed very consequently especially where in modern economies trade in abstract instruments has come in place of trading concrete goods. In German law it is nearly an exception that a transaction demands documentary evidence. Instead, often good faith in the public outward appearance is protected. On the other side we find a strong emphasis on publicity in modern company law with the liability of companies to publish their yearly balances or the liability of shareholders to give notice, when they have gained a certain power in the company after having acquired a certain fraction of its shares.

¹⁹ To which extent these principles hold for obligations is questionable at the least; but such doubts do not concern intellectual property.

Insistence on publicity of legal relations and transactions is no pure formalism. Publicity means perceptibility of the legal state of affairs. Publicity is indispensable to evaluate the risks when one engages in dealing with business partners. Lack of publicity of the real financial standing is perhaps the main reason for losses, when a business partner goes bankrupt. But far more important is perhaps that our general freedom of action depends on the ability to recognize when we get to do with rights of others and are in danger to interfere with these rights. This danger is not too big when it comes to chattels or land, since we know that, if an object is not our own, it most likely belongs to somebody else. There is even less danger in the case of debtor- creditor-relations where we generally are not in a position to interfere with the relations of third parties.

This seems to be different with intellectual property. Surely, one should be warned, when one finds an efficient machinery and intends to start an own business with a reproduction of that machinery. As well, it should be unnecessary to tell people that they must not maintain something to be their own creation if they have copied it from a foreign source.

Specificity and publicity as general principles and patent and copyright as intellectual property rights do not exhaust the whole set of problems but might suffice as a starting point to exemplify now the question how intellectual property rights might relate to general principles governing subjective rights.

2.3. Patent

Patents are granted for inventions. An invention is a solution to a specific technological problem, and may be a product or a process.²⁰ To be patentable mainly three conditions have to be met: The invention must offer something new, useful, and non-obvious.²¹ But these criteria alone do not give a clear guidance for a decision about eligibility for a patent.

a) Patents in Genes

Lately in a case decided by the Supreme Court of the United States (SCOTUS) the question had to be answered, whether a patent for isolated genes claims protection for a new and useful composition of matter or whether it claims a right in a naturally occurring phenomenon²². Genes are a product of nature, and the Supreme Court had long held that laws of nature, natural phenomena, and abstract ideas are not patentable.²³ But at once the Court narrowed this principle:

The rule against patents on naturally occurring things is not without limits, however, for “all inventions at some level embody, use, reflect, rest upon, or apply laws of nature, natural phenomena, or abstract ideas,” and “too broad an interpretation of this exclusionary principle could eviscerate patent law.”²⁴

Here we find a statement that can be referred to the postulation above that access to information is access to reality, to real naturally occurring things and that in an enlightened pluralistic democratic society no obstacle induced by law may bar access to reality. This means that under the premise that all natural phenomena must be exempt from patent there cannot be any patents at all. The converse argument would be: Only for unnatural phenomena a patent could be claimed, and this would be absurd.

²⁰ So, Wikipedia s.v. Patent.

²¹ US Patent Act – 35 USCS § 101 ss.

²² Association for Molecular Pathology et al. v. Myriad Genetics, Inc., et al., 569 U. S. ____ (2013). [http://www.supremecourt.gov/opinions/12pdf/12-398_1b7d.pdf]: Myriad had discovered the precise location and sequence of two human genes, mutations of which can substantially increase the risks of breast and ovarian cancer.

²³ The Supreme Court referred to its earlier decision in Mayo Collaborative Services, DBA Mayo Medical Laboratories, et al. Petitioners v. Prometheus Laboratories, Inc., 566 U.S. ____ (2012).

²⁴ SCOTUS in Myriad with reference to Mayo.

The Supreme Court does not solve this dilemma; it turns its argumentation to a practical criterion:

As we have recognized before, patent protection strikes a delicate balance between creating incentives that lead to creation, invention, and discovery and impeding the flow of information that might permit, indeed spur, invention. We must apply this well-established standard to determine whether Myriad's patents claim any new and useful . . . composition of matter, or instead claim naturally occurring phenomena.²⁵

This sounds sensible, though the Supreme Court here takes on a role that is not based on law. The Supreme Court sees itself in a political role with the decision, either to keep an information free to further scientific research or to give the power to dispose of scientific information into the hands of a monopolist. In the wording of the opinion of the Court this decision is the standard to determine whether the patent claim fulfills the conditions of novelty and usefulness of the composition. Perhaps, the other way round the argumentation would sound more persuasive: Novelty and usefulness as standard for acceptance as a patent. This would get support from the text of § 101 Patent Law: "Whoever invents or discovers any new and useful composition of mattermay obtain a patent ...". Novelty and usefulness then decide whether to give a monopoly or not. In the case of discoveries novelty and usefulness alone are not sufficient for patentability: "Groundbreaking, innovative, or even brilliant discovery does not by itself satisfy the §101 inquiry."²⁶ Demanded is that the patent claim is "not to a hitherto unknown natural phenomenon, but to a nonnaturally occurring manufacture or composition of matter—a product of human ingenuity 'having a distinctive name, character [and] use'".²⁷

Actually, the Supreme Court had to decide not only one patent claim but two different claims. With one Myriad claimed a patent for isolated genes, with the other it claimed a patent for a modified gene, the so-called composite DNA (cDNA), "which contains the same protein-coding information found in a segment of natural DNA but omits portions within the DNA segment that do not code for proteins."²⁸ In the outcome the Supreme Court abolished the patent for DNA but approved the patent for cDNA. The decisive criterion became the question whether the subject matter of a patent did exist in nature as such or had been modified (under the conditions of novelty, usefulness) by the applicant. The Supreme Court saw these conditions as given with cDNA.

Critical comments immediately after publication of the decision have maintained that cDNA was as much a part of nature as DNA. And, indeed, cDNA does not constitute a new composition of matter but is arrived at by decomposition of DNA, rather, by omitting portions of the DNA segment.

Apparently the clear distinction what makes a subject matter eligible for patent remains a conundrum. A comment on the decision of the Supreme Court in a German newspaper states bluntly: In patent law the so-called common sense encounters its limits.²⁹

b) Patent and specificity

This predicament can give cause to approach the question where the problem can be localized from the viewpoint of traditional legal standards. And ideas like "incentive for further research", "reward for creativity" or the remuneration of labor ("the sweat of the brow") do not belong to such legal standards.

If as a starting point is taken the general principle that only individual, specific things (things in the broadest sense) can be subject matter of a subjective right: Will this help to distinguish between

²⁵ SCOTUS in Myriad, *ibidem*; quotationmarks omitted.

²⁶ SCOTUS in Myriad, Opinion p.12

²⁷ *Ibid.*

²⁸ *Ibidem*, Opinion p.1.

²⁹ „Der sogenannte gesunde Menschenverstand stößt im Patentrecht an seine Grenzen.“, *Jörg Albrecht* in: *Frankfurter Allgemeine Sonntagszeitung*, June 16, 2013, p. 55.

phenomena eligible for patent and such that are not? It should be kept in mind here, that it is not the machine itself that incorporates the patent or the concrete work in progress that is protected by the patent; protected is the underlying description of the machine or of the method, such as it has been filed at the patent office. This description contains an information about something real, a phenomenon of the real world. This information is always general, one would not get a patent for a single incidence; it is understood that the phenomenon specified by the patent description has to be reproducible. It then is never specific in the sense demanded by the principle of specificity for the subject matter of a subjective right.

The outcome under the principle of specificity is here the same as the concerns of the Supreme Court reported above. There the Court considered that all inventions lastly rest upon laws of nature, natural phenomena, or abstract ideas and that a rigorous adherence to such reasons for exclusion would jeopardize patent rights generally. The principle of specificity then stands in the way of any patent rights.

However, principles in law are not as rigorous as laws in natural sciences. Principles in law will be better understood as standards to be followed and indicating, when an irregularity demands special consideration and substantiation. And it can be shown that this consideration seems to have guided modern patent law, whether consciously or not. Even a concern might be perceived to keep the intrusion into standards as small as possible.

Generally subjective rights as a standard have no expiration date (which counts for another general principle). As an irregular right patent is limited in time, to a term of 20 years in most countries. The patent right of somebody else does not hinder anybody to make use of it, to develop it further or to communicate it to others. The patent right blocks only the commercial use of the patent by others than the patent holder not its information. In German law consequently it appears under the heading of gewerbliches Schutzrecht (commercial protection right).

c) Patent and Publicity

One can be short about patent and publicity: What is most important under the aspect of a right to know, to have access to knowledge and information: Patent law provides perfectly for this right. A patent is awarded only if its relevant information is published in the patent description that has to be filed and is accessible at the patent office.

d) Limitation of patent

If patents generally only can be granted by intrusion into the principle of specificity, the question remains why then should there at all remain an area that has to remain free of patents. The endeavour of the Supreme Court to draw the line between patentable and not patentable phenomena then might seem futile. But the whole legal discussion rests on the conviction that there must be boundaries for patents, and this is what common sense demands. It will not help much to weigh the interest of inventors and the interest of the public against each other. Such weighing will not bring about a clear decision, it just shows the concurring, antagonistic interests of the parties and the propensity of the decision maker to let one prevail over the other. Legal science is challenged to find a distinctive criterion.

e) Scarcity

Indeed, the problem of such a distinction is not new at all in jurisprudence. The preußische Allgemeine Landrecht (the General State Laws for the Prussian States) of 1794 contained a rule that might be understood to render the distinction as it is handled by the Supreme Court giving it a more general reach, by covering rights generally: "Things of such a nature that nobody can be excluded

from their use, cannot become property of individual persons.”³⁰ This rule shows in its essence only another dimension of the principle of specificity.

One might go so far as to reformulate this dimension of specificity into a new principle: Things that are not diminished by use or participation of anybody cannot be subject matter of a subjective right, or: Subject matter of a subjective right can only be something that is or can become scarce. This principle supports the argumentation of the Supreme Court. DNA is given by nature, it is generally not scarce, how difficult it might be to isolate it. cDNA as a modification or alteration of DNA must be produced, it demands the investment of labour. So, it can be diminished and can potentially become scarce. The qualification for a subjective right here meets the definition of goods in economy, which demands scarcity of an item.³¹

To return now to the problem of subjective rights in knowledge: Knowledge and information are not scarce after they once have been created. They can be multiplied endlessly, they are not diminished by use and participation of others, on the contrary, they are augmented thereby. So, there should not exist subjective rights in knowledge or information.

2.4. Copyright

a) Scarcity

The conclusion that something that is not scarce, that can be multiplied endlessly and is not diminished by the use and participation of others cannot be subject matter of a subjective right applies as well to the copyright. The term “copyright” – much clearer than Finnish “tekijänoikeus” or German “Urheberrecht” – shows explicitly that the protected matter can be multiplied without any considerable loss, though the act of copying might demand expenses. The subject matter of the copyright is no scarce good, it is artificially made scarce by the copyright. The, in principle copyrighted material is no suitable subject matter for a subjective right. As an exception the copyright consequently must be limited to a narrow range, where it does not conflict with the free access to knowledge and information.

Reservations of legislators as to the extent of the copyright can be found in the beginning of codified copyright law in the 18th century. In England in 1710 in the Statute of Anne, the world’s first codified copyright, the term of protection was 14 years after publication. In the United States the first federal copyright act granted protection for 14 years as well (after registration) with the possibility of renewal for 14 more years if the author survived the first term. In France a general copyright law limited the protection to ten years after the death of the author. In Germany Prussia and the “Federal assembly” (Deutscher Bund) decided to give copyright protection for ten years after publication, a term that later was prolonged to 30 years after the death of the author. The Berne Convention of 1886 then fixed a term of 50 years.

b) Specificity/Scarcity

As a mitigation of the irregularity of the copyright as a subjective right might be seen the traditional rule that it is only the form, the expression of a production that can be protected by copyright, not the content. This seems to go parallel with the distinction between invention and discovery, as handled by the Supreme Court. The form of an utterance in art or literature is an invention, a creation of the author, the content is something given by reality or found in nature, discovered in a sense. This simple rule seems plausible and it satisfies the condition that only specific phenomena can be subject matter of a subjective right. The content as observable and intended to be reproducible in reality

³⁰ pr. ALR 1. Theil, Achter Titel § 3: „Sachen, von deren Benutzung, ihrer Natur nach, Niemand ausgeschlossen werden kann, können kein Eigenthum einzelner Personen werden.“

³¹ Cf. Stephan Kinsella, Against Intellectual Property, *Journal of Libertarian Studies* 15(2):1–53 (2001).

and thus is in the range of knowledge and information cannot be monopolized by a subjective right. Content lacks specificity. The expression of an idea is something that did not exist before creation; it is specific and may be reserved to the author.

There are cases where it seems doubtful whether this distinction between form and content can be followed strictly. In literature or any other art with a fictitious plot one might doubt whether the characteristics of the plot belong to expression or whether they are content of a work. But the distinction works well in most cases and still governs the general understanding of copyright. So, the Directive 2009/24/EC of the European Parliament and the Council of 23 April 2009 as well as its predecessor of 1991³² on the legal protection of computer programs emphasizes in its recital:

“(11) For the avoidance of doubt, it has to be made clear that only the expression of a computer program is protected and that ideas and principles which underlie any element of a program, including those which underlie its interfaces, are not protected by copyright under this Directive. In accordance with this principle of copyright, to the extent that logic, algorithms and programming languages comprise ideas and principles, those ideas and principles are not protected under this Directive. In accordance with the legislation and case-law of the Member States and the international copyright conventions, the expression of those ideas and principles is to be protected by copyright.”

This commitment to the traditional distinction between expression and content can be seen as a pure hypocrisy. It is this directive that sets requirements for protected expression at so low a level that in the outcome the content of the software itself gets copyright protection. Recital (8) of the directive states accordingly:

“In respect of the criteria to be applied in determining whether or not a computer program is an original work, no tests as to the qualitative or aesthetic merits of the program should be applied.”

Evidently not the expression but content is protected when it is not only the computer program itself that is copyrighted, but the preparatory material as well

“...This term (sc. Computer program) also includes preparatory design work leading to the development of a computer program provided that the nature of the preparatory work is such that a computer program can result from it at a later stage.”³³

What qualifies preparatory work for copyright here is not its expression or form, but its function. Under such premises it will be hard to find any example of computer software that does not qualify for copyright protection under this directive.

Generally during the last decennia a strong tendency can be observed to extend the copyright to domains where it traditionally did not belong or that were out of the scope of copyright. A prominent role in this process has played the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) of 1994. This Agreement demands from all member states of the World Trade Organization (WTO) to enact protection for phenomena irrespective of their expression that are clearly to be understood as content. Among these phenomena are products such as sound recordings and broadcasting, industrial design, integrated circuit lay-out designs (so-called mask work), patents, plant varieties, trademarks, geographical indications, confidential information, and others.

The extensions apparently strive to award increasingly copyright protection to content, abandoning the traditional distinction between expression eligible for copyright and content that must remain free. This tendency has gained harsh critique world-wide as being lopsided in the advantage of interested, powerful lobbying groups in the industries. One of the gains from copyright protection for

³² Directive 250/1991/EC.

³³ Cf. Recital (7) and art. 1 para.1 of the Directive.

them is that there is no correction by such criteria as they govern patent law – i.e. that the content has to be new, useful and non-obvious.

The considerateness which was observable in patent law apparently has had no place in copyright law. The incentive for awarding copyright protection seems to be the expectation of gains by a monopoly for goods where consumer demand is presumed. The oddity that by copyright in intellectual property a good that exists in unlimited amount (or: that are “non-excludable” and “non-rival” in economic terms) is monopolized has long been noticed in the economic discussion. Such goods are characterized as artificially made scarce.³⁴ One should doubt whether it can be a task of law to make its instruments available to endeavours to make things scarce that are unlimitedly at everybody’s disposition.

To include scarcity into the inventory of legal principles does not mean to exclude copyright generally. As in the case of patents one could argue that as a principle scarcity is open for modification. The aim is to prevent that access to knowledge and information about the real world is barred. This concerns content not expression. Expression is or at least can be specific; it can be individualized as a certain creation, named by the author and its manifestation in a piece of literature, music or art. It can be copied, but is not reproducible. In this sense it can be scarce and subject matter of a subjective right.

c) Publicity

The principle that subjective rights must somehow be made public is no problem if for the formation of the copyright some kind of publication is demanded. In modern copyright law, however, the copyright comes into existence already by the act of creation. Publication is not demanded, it is enough that the work has got an observable manifestation which has not to be public.³⁵

Since copyright originates with the act of creation already, it seems to make an exception to the principle that subjective rights need to be public in some way. This would be no problem if it is only the expression that has the copyright and not the content or idea of the work. The monopolization of an expression, leaving the content free cannot be an intrusion into the right of access to knowledge and information.

This waiver of publicity is unacceptable if the borderline between expression and content is exceeded and the protection of copyright is given to phenomena belonging to the real world. A telling example for such an excess is again the Council Directive 91/250/EEC cited above.

One can look at it as a masterpiece of legislative obscurity how in the articles 4 – 6 of this directive publicity of copyrighted matter is foreclosed. Under the heading “Decompilation” is regulated under what condition it is allowed to have a look at the matter of a copyrighted computer program. Paragraph 1 of article 6 renders the conditions:

“The authorisation of the rightholder shall not be required where reproduction of the code and translation of its form within the meaning of points (a) and (b) of Article 4(1) are indispensable to obtain the information necessary to achieve the interoperability of an independently created computer program with other programs, provided that the following conditions are met:

- (a) those acts are performed by the licensee or by another person having a right to use a copy of a program, or on their behalf by a person authorized to do so;
- (b) the information necessary to achieve interoperability has not previously been readily available to the persons referred to in point (a); and

³⁴ For evidence browse the internet s.v. „artificially scarce good”.

³⁵ Beyond that, Common Law demands that this manifestation has to be in some material form. The difference is not too big and concerns mainly the copyright in speeches and other performances.

(c) those acts are confined to the parts of the original program which are necessary in order to achieve interoperability.”

In clear words this means: Generally it is forbidden to have a look at the content of a computer program without permission by the rightholder. For a very limited aim, to achieve interoperability, not the public but only a person who has a right to use the program may look at the code of the program. But even this person is not free to use the knowledge he has acquired. Paragraph 2 of art. 6 binds him:

“The provisions of paragraph 1 shall not permit the information obtained through its application:

(a) to be used for goals other than to achieve the interoperability of the independently created computer program;

(b) to be given to others, except when necessary for the interoperability of the independently created computer program; or

(c) to be used for the development, production or marketing of a computer program substantially similar in its expression, or for any other act which infringes copyright.”

In this paragraph it is made explicit that it is information, knowledge, content that is copyrighted and hidden from the public. Under letter (c) then a reminiscence of copyright rules seems to have worried the lawgiver, when besides other acts which infringe copyright the information may not be used for a computer program “substantially similar in its expression”. This return to expression as a criterion traditionally governing copyright law is mere hypocrisy after in letter (a) it is already forbidden to use the information for other goals than to achieve interoperability.

As a subjective right the so-called software directive has created a legal monster. This should worry the legal profession. Perceptibility and publicity of the subject matter of subjective rights are indispensable in private law. In copyright law they are the condition that not only concurring programmers, but authors generally can avoid infringements of a copyright and avoid possible disputes about copyright. But generally they make the legal world visible and manageable and thereby guide *freedom of knowledge and information*.

IDENTITY THEFT AND THE FINNISH IDENTITY PROGRAMME

Rauno Korhonen

Professor of Legal Informatics, University of Lapland, Faculty of Law,
Institute for Law and Informatics, P.O.Box 122, FI-96101 Rovaniemi, Finland
rauno.korhonen@ulapland.fi; www.ulapland.fi

Keywords: *Identity theft, cybercrime, information offence, privacy, data protection, information security.*

Abstract: This paper analyses identity theft as one form of modern cybercrimes. There are different kinds of identity theft and their existence and type is often dependent on the country and legal culture involved and the information technology or information systems. Finland has been working on a programme (known as the Finnish Identity Programme) for a number of years to combat identity theft. The paper will take up the principal issues addressed by the Programme and present the memorandum of the Ministry of Justice assessing the work of the Programme.

1. Introduction

Different kinds of cybercrimes¹ or information and communication offences, are everyday occurrences nowadays.² One possible target for such criminal activities is a person's identity.³ Indeed, identity thefts have become a serious matter in the modern world. Several countries have already taken substantial measures to prevent identity thefts. It is assumed that the situation will deteriorate from its current state, with Finland being no exception to this trend.

¹ One possible definition for cybercrime is the following: "Cybercrime can be regarded as computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks. Its distinctiveness is derived from the versatile capabilities provided by the new ICTs." See *Thomas, Douglas/Loader, Brian D.*, Introduction, p. 3.

² A very new piece of research in this field is *UNODC*, Comprehensive Study on Cybercrime. Draft – February 2013 (320 pages). *UNODC* is the United Nations Office on Drugs and Crime. This study observes (p. 99): "At the national level, country responses to the Study questionnaire show that comparatively small proportion of countries – 25 per cent – report the existence of a cyber-specific provision for identity-related offences." *UNODC* has also published in 2011 Handbook on Identity-related Crime.

³ In this context, identity as a concept should have been explained and analysed in more detail. However, in this short paper it is not possible and necessary. We have enough literature concerning the concept, for instance *Stuart Hall's* well-known study *Identity*. Moreover, some researchers have recently begun to talk about a concept of and our new right to a digital identity. See, for example: *Monteleone, Shara*, Privacy and Data Protection at the time of Facial Recognition: towards a new right to a Digital Identity? *European Journal of Law and Technology*, Vol. 3, No. 3 (2012). *Monteleone* writes (p. 16-17): "Often digital identity protection is associated almost exclusively with identity theft (i.e. obtaining information to commit a fraud, linked usually to financial issues), but digital identity is something more and different. It does not necessarily coincide with privacy and data protection (i.e. identity protection may be not ensured even though privacy and data protection rules are respected) and, as sustained in this paper, it should be conceived more as the right to the free and untracked building and representation of one's own personality – as a 'digital persona'."

Serious cases have been reported in Finland regularly in recent years. In November 2011, the National Information Security Agency (CERT-FI) reported, that the personal data of more than 16,000 people had leaked on to the Internet. A couple of weeks later, our TV news reported that a list containing the e-mail addresses of some 500,000 Finnish people could be found and accessed freely on the Internet. Similar cases are regrettably common; they appear almost every week in Finland and everywhere in the industrialised countries. In all likelihood, many cases receive no publicity, because not all data leaks are reported. Bad news is certainly not good PR for the information security units of private companies or public sector authorities.

Preventing this kind of criminality will require that we consider both national and international measures. Citizens' trust in the information systems of both the private and public sectors is necessary. One useful approach would be international police co-operation. Recently, the European Commission decided to establish a *European Cybercrime Centre (EC3)*.⁴ The Centre will be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. It will support Member States and the institutions of the European Union in building operational and analytical capacity for investigations and cooperation with international partners. The EC3 is hosted by Europol, the European law enforcement agency in The Hague.⁵

In March 2013, for the first time in Finland, all the ministries and the Office of the President of the Republic conducted a national exercise to prepare for a large cyber attack. This exercise consisted of, among other things, analysing different kinds of threats, risks and vulnerabilities. The Finnish Government says that cyber security is a new area of defence. Most of the material produced in conjunction with the exercise is secret and classified but due to the principle of openness of the democratic state the main issues addressed in such an activity by an authority must always be published.⁶

The EU and many countries are now developing their legislation and cyber-strategies.⁷ In January 2013, Finland published its *Cyber Security Strategy*, which defines the key goals and guidelines to be used in responding to threats against the cyber domain and which ensure its functioning. By following the guidelines in the Strategy and the measures required therein, Finland can manage deliberate or inadvertent disturbances in the cyber domain as well as respond to and recover from them.⁸

One of the guidelines in the Strategy is that the Finnish police should have sufficient capabilities to prevent, expose and solve cybercrimes. Another is that the preconditions for the implementation of effective cyber security measures should be ensured through national legislation. Cybercrimes are a technically and legally challenging field. In Finland, only few specialists among the pre-trial

⁴ Earlier, in 2004, the EU established *ENISA*, the European Network and Information Security Agency, which works for the EU Institutions and Member States. See www.enisa.europa.eu.

⁵ See: <https://www.europol.europa.eu/ec3> (A collective EU response to cybercrime).

⁶ Finnish Government's webpages (11.3.2013): <http://valtioneuvosto.fi/ajankohtaista/tiedotteet/tiedote/fi.jsp.print?oid=379019> (press release only in Finnish and Swedish).

⁷ See European Commission's Proposal for a Directive of the European Parliament and of the Council on attacks information systems and repealing Council Framework Decision 2005/22/JHA. Brussels, 30.9.2010. COM (2010) 517 final. See also European Commission's Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union. Brussels, 7.2.2013. COM (2013) 48 final.

⁸ Finland's Cyber Security Strategy has been adopted. The Ministry of Defense's webpages can be found at <http://www.defmin.fi>, Press Releases 24.1.2013 (en). The text of the Strategy can be found translated into English at: <http://www.yhteiskunnanturvallisuus.fi/en>

investigators, prosecutors and judges have sufficient knowledge in the fields.⁹ The extensive legislative reform of the Pre-trial Investigation Act, the Police Act and the Coercive Means Act, will enter into force on 1 January 2014. This new set of laws will mean further challenges for education.

In order to stop attacks, cyber-strategies often concentrate also on countering active cyber-attacks, not only on defence systems. The United States Government recently revealed that it has established its own cyber-warfare unit for the US Army. This unit, *Cyber Command*, has 40 subgroups, 13 of which are specialised in cyber-attacks. If the US is attacked, the unit is ready to launch a counter cyber-attack.¹⁰

2. Identity Theft as a Concept

Several definitions of the concept of identity theft can be cited. For example, one states: “*Identity theft is a form of fraud or cheating of another person’s identity in which someone pretends to be someone else by assuming that person’s identity, typically in order to access resources or obtain credit and other benefits in that person’s name.*”

The victim of identity theft can suffer adverse consequences if he or she is held accountable for the perpetrator’s actions. In some cases, the victim is obliged to change his or her entire identity, name and personal identification number, because the original identity has been placed in a negative light by criminal use. Organisations and individuals who are duped or defrauded by an identity thief can also suffer adverse consequences and losses, and to that extent are victims.

The term “identity theft” is actually a misnomer, because it is perhaps not literally possible to steal an identity as such. More accurate terms would be *identity fraud* or *identity cloning*. But “identity theft” has become commonplace in the modern discussion. Identity fraud is often, but not necessarily, the consequence of identity theft. Someone can, of course, steal or misappropriate personal information (data) without subsequently committing identity theft by using the stolen information; this is the case, for example, in the aftermath of a major data breach.

3. Some Examples of Identity Thefts

In international literature identity theft has been divided into several possible subcategories, among them: *identity cloning and concealment*; *criminal identity theft*, *synthetic identity theft*; *medical identity theft* and *child identity theft*. The concepts, terms and subcategories vary considerably depending on the particular studies and papers.¹¹ I will present briefly only some examples.

In *identity cloning and concealment*, the identity thief impersonates someone else in order to conceal the thief’s own true identity. Typical cases of this kind pertain to illegal immigrants, people hiding from creditors or other individuals who simply want to become anonymous for personal reasons.

⁹ In Finland only two legal doctoral theses have been written in the field of cybercrimes (or data and communication offences). The first of the authors, a former prosecutor, has passed away, and the second one, originally from China, is not working in Finland anymore.

¹⁰ See “USA paljasti kybersotasuunnitelmansa – ”Iskemme hyökkääjiä vastaan verkossa”. (“The USA reveals its cyber war plan – We’ll attack the attackers on the Net”), www.iltasanomat.fi (14.3.2013).

¹¹ See for instance: *Van der Meulen, Nicole/Koops, Bert-Jaap*, The Challenge of Identity Theft in Multi-level Governance. Towards a co-ordinated action plan for protecting and empowering victims. TILT Law & Technology Working Paper No. 013/2009. See also *Cheney, Julia S.*, Identity Theft: Do Definitions Still Matter? Discussion Paper. Payment Cards Center. August 2005. Federal Reserve Bank of Philadelphia. www.phil.frb.org

Another example is *posers*, a label given to people who use somebody else's photographs and information on social networking sites. For the most part, posers create believable stories involving friends of the real person they are imitating. Unlike identity theft – which when committed for the purpose of obtaining credit, usually comes to light when debt mounts, – *concealment* may continue indefinitely without being detected, particularly if the identity thief is able to obtain false credentials in order to pass various authentication tests in everyday life.

When a criminal fraudulently identifies him- or herself to police as a different individual upon arrest, it is sometimes referred to as *criminal identity theft*. In some cases, criminals have obtained state-issued identity documents using credentials stolen from others, or have simply presented false identification documents. Provided the perpetrator succeeds, charges may be filed under the victim's name, letting the criminal off the hook. It can be difficult for the victim of a criminal identity theft to clear his or hers records.

In *synthetic identity theft*, identities are completely or partially fabricated. The most common technique involves combining a valid social security number with a name and birthdate other than the ones properly associated with the number. Synthetic identity theft is less likely to be exposed, as it does not show on a person's credit report directly, but may appear either as an entirely new file in the credit bureau or as a subfile on one of the victim's credit reports. Synthetic identity theft primarily harms creditors who unwittingly grant the fraudsters credit.

Medical identity theft occurs when someone uses a person's name and sometimes other parts of his or her identity – for instance insurance information – without the person's knowledge or consent in order to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, which may in turn lead to inappropriate and potentially life-threatening decisions by medical staff.

Child identity theft occurs when a minor's social security number is used by another person for the imposter's personal gain. Social security numbers, and other personal identification numbers in general, are valued, because they usually do not have any information associated with them. Thieves can establish lines of credit, obtain driver's licences, or even buy a house using a child's identity. This fraud can go undetected for years, as most children do not discover the crime until years later.

There are certainly some differences among identity thefts, depending on the culture, technology and legal systems involved. The categories of theft described above are probably easier to commit in the US and in certain other countries where no centralised, nationwide population data register or digital system exists. As far as I know, for example, in the US the social security numbers and car registration numbers in use in each of the states differ from each other.¹² In the Nordic countries, identification systems and documents are based on nationwide, electronic population data registers. Each citizen has only one, unique personal identification code, which consists of the date of the birth and a unique technical code. This means that two citizens, born on the same day and in the same year, cannot have the same code. The processing of personal data and codes is also strictly regulated by data protection legislation. In Finland, the official personal identification code (fi *henkilötunnus*) has been used in the

¹² See the discussion in the USA for instance: Steinbock, Daniel J., Fourth Amendment Limits on National Identity Cards. In Strandburg, Katherine J./Stan Raicu, Daniela (editors): Privacy and Technologies of Identity. A Cross-Disciplinary Conversation, Springer, USA 2006. See also the webpages of Internal Revenue Service of the United States Government: <http://www.irs.gov>. The IRS is committed to protecting the privacy rights of America's taxpayers. It has its own Privacy Policy and special pages providing guidance for identity theft victims.

public and private sector since the 1960's. Other identification numbers have only a secondary role. Stealing identities and making false documents should be much more difficult – but not impossible, of course.

4. Identity Theft as a Crime in Finland

Chapter 38 of the Finnish Criminal Code contains the main provisions on data and communication offences. The first sections came into force in 1995, and several amendments have been enacted since. An extensive reform of the legislation was carried out in 2007, when the rules of the *EC Cybercrime Convention* were taken into consideration. Other rules concerning so-called cybercrimes can be found in other chapters of the Criminal Code.¹³

Chapter 38 of the Finnish Criminal Code; Data and communications offences:

Section 1	Secrecy offence (578/1995)
Section 2	Secrecy violation (578/1995)
Section 3	Message interception (531/2000)
Section 4	Aggravated message interception (578/1995)
Section 5	Interference with communications (578/1995)
Section 6	Aggravated interference with communications (578/1995)
Section 7	Petty interference with communications (578/1995)
Section 7 a	Interference in a computer system (540/2007)
Section 7 b	Aggravated interference in a computer system (540/2007)
Section 8	Computer break-in (578/1995)
Section 8 a	Aggravated computer break-in (540/2007)
Section 8 b	Offence involving an illicit device for accessing protected services (540/2007)
Section 9	Data protection offence (525/1999)
Section 10	Right to bring charges (578/1995)
Section 11	Forfeiture (1118/2001)
Section 12	Corporate criminal liability (540/2007)

Currently, writing under the name of another person is not a crime in Finland if the content is not actually libellous, or if economic fraud is not involved.¹⁴ To date the Ministry of Justice has taken the view that no legislative changes are needed, as the most serious types of identity theft, such as making purchases in someone else's name, are already crimes. However, in an interview given in 2011, the Data Protection Ombudsman of Finland, *Reijo Aarnio*, stated that identity theft as such should be criminalised, regardless of whether or not monetary gain is involved.

¹³ In addition to these provisions, the Finnish Criminal Code contains provisions on offences such as endangerment of data processing (CC 34:9 a); possession of a data system offence device (CC 34:9 b) and preparation of means of payment fraud (CC 37:11). See www.finlex.fi/en/laki/kaannokset/ or www.finlex.fi > Translations of Finnish acts and decrees > Criminal Code (39/1889).

¹⁴ However, according to chapter 16, section 5 of the Finnish Criminal Code, presenting oneself to a public authority/civil servant using another person's identity is punishable. This rule is not applied if the person presents him- or herself to an ordinary citizen using false identifying information. In general, the misuse of personal data of another person has been criminalised in several ways in Finnish legislation.

5. The Finnish Identity Programme

In 2008, the *Ministry of the Interior* of Finland established a working group to draw up what was to be known as the *Identity Programme*. The report of the working group was published in 2010.¹⁵

The working group saw the practice of identity theft as a significant problem. According to the report, identity thefts are criminal actions in which information about people's private identity is collected and used with a purpose to:

- gain great illegal financial benefit;
- violate the rights of the original identity owner; or
- violate the constitutional rights of the original identity owner without the purpose of seeking concrete benefits or without an intention to harm the original identity owner.

The report further notes that "*the government has an obligation to protect a person's identity to the same degree in both electronic and physical operational environments.*" The working group also analysed these environments and said that identity thefts committed in physical environments are isolated cases, and that in this area, the crime prevention authorities normally have sufficient resources. Identity thefts committed in electronic environments are more difficult. In that area, the pre-trial investigators are often not competent to investigate all of the facts, for example, because they lack sufficient technical knowledge.

The aim of the working group was to create an identity programme, which would present the current state of identity creation as well as views on future development and the risks involved. An additional aim was to present conclusions and recommendations for future actions. The focus of the analysis was on the government's role in creating an identity for an individual in Finnish society, and on the methods with which the state protects its citizens' identity against identity thefts in both national and international operational environments.

In the course of the project, the working group collected essential terms in the field of identity thefts and gave them definitions. Its report covered different identification methods, certificates and identification documents, and risks involved. It also explained biometry and its development in Finnish law enforcement and examined reformed legislation on identity issues.

One of the main functions of the working group was to carry out a practical survey of Finnish citizens' views on potential threats in the field of identity thefts and then examine these problems and the victims' status. Many parties in Finland have suggested that identity thefts should be criminalised, but we still lack a detailed analysis of the matter. Accordingly, the report specified different types of criminalisation and pinpointed the problem zones to build a base and provide support for prospective further actions.

The working group formulated the following concluding remarks concerning identity thefts¹⁶:

- 1) Using another person's identity limits the victim's personal self-determination;
- 2) A victim's position is weak during the crime investigation process;

¹⁵ *Ministry of Justice*. Publications Series 32/2010. (Available only in Finnish and Swedish.)

¹⁶ Identity theft was not the only topic or theme assigned to the working group. It also dealt with issues concerning the driving license as an identification document, a unified procedure for providing passports and other identification documents, revocation lists for driving licenses, identification cards and passports and the need for new legislation on biometric identification applications.

- 3) A centralised notification system is necessary for the victims of identity theft;
- 4) An advisory committee for identity security should be established;
- 5) Guidelines for identity theft victims should be written;
- 6) A new working group must be appointed in the near future.

The group was not actually proposing that identity theft should be criminalized; it left the matter for the *Ministry of Justice* to consider. The next step would be to create a new working group to examine the issues raised in the identity programme report. The Ministry of Justice should convene the new working group, which should concentrate on examining the following legislation:

- Provisions in the Finnish Criminal Code
- Provisions in the Finnish Constitution; and
- Provisions in other essential legislation in the area of identity and the influence of legislation on the status of victims.

In March 2013, the Ministry of Justice of Finland published an assessment memorandum¹⁷, which includes an evaluation of the report of the Identity Programme as well as some proposals for future actions.

As a concluding remark, the Ministry of Justice states that there does not exist only one typical criminal offence that we could call “identity theft”. In a broader sense, identity theft could mean all kinds of collecting of personal data or using of another person’s name. The criminalising of all the actions would easily lead to excessively vague and unclear criminalisation, if we consider the *legality principle*. The Ministry of Justice reports that the current national legislation and the new legislation which will come into force in the near future, are mostly relevant and sound, as far as the remit of the Ministry is concerned.

The Ministry of Justice agrees with the working group that the instructive and preventive measures, as well as effective remedial measures after the crimes have been committed, are very important in dealing with identity thefts. Criminalisation should be restricted and the criminal law should always be the last resort (*ultima ratio*).

6. Conclusion

In January 2012, the EU Commission published a proposal for a new Personal Data Protection Regulation.¹⁸ The current EU Personal Data Directive will probably be replaced by the new regulation, and national legislation in the member states will be reformed. Because of the hierarchy of laws in the EU, it is possible that national data protection acts will become unnecessary in the future. At the same time, a proposal for a new directive was given.¹⁹ The new regulation and this directive will together form an extensive reform of EU data protection legislation.

¹⁷ See: *Ministry of Justice*, Identiteettivarkaus; henkilöllisyyden luomista koskevan hankkeen (identiteettiohjelma) työryhmän loppuraportin arviointia ja ehdotuksia jatkotoimiksi. Arviomuistio. Oikeusministeriö 15.3.2013 (OM 4/41/2013). (This paper is available only in Finnish and Swedish.)

¹⁸ See 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). Brussels, 25.1.2012. COM (2012) 11 final.

¹⁹ See Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. Brussels, 25.1.2012. COM (2012) 10 final.

In its assessment memorandum the Ministry of Justice mentions several times the proposal for a directive on attacks against information systems.²⁰ After the transposition process and harmonisation with the Finnish legislation, the new directive will be important, because it includes provisions concerning the use of another person's identity information when committing crimes.

Our legislation concerning criminal investigations and the police authorities has undergone a substantial reform. The new laws: the Police Act (872/2011), the Pre-trial Investigation Act (805/2011) and the Coercive Means Act (806/2011) will enter into force on 1 January, 2014. These acts will assign new powers for applying the measures to prevent and investigate identity thefts and other cybercrimes.

For these and the other reasons mentioned in the assessment memorandum, the Ministry of Justice of Finland is reluctant to go on working with the Identity Programme at this moment. We are first waiting for the results of the new EU legislation and experiences in applying the new laws.

7. References

Bewerley-Smith, Huw, *The Commercial Appropriation of Personality*. Cambridge Studies in Intellectual Property Rights. Cambridge University Press 2005.

Cheney, Julia S., *Identity Theft: Do Definitions Still Matter?* Discussion Paper. Payment Cards Center. August 2005. Federal Reserve Bank of Philadelphia. www.phil.frb.org

Gilliot, Maïke/Matyas, Vashek/Wohlgemuth, Sven, *Privacy and Identity*. In Rannenberg Kai, Royer Denis and Deuker André (editors): *The Future of Identity in the Information Society. Challenges and Opportunities*. Springer. Berlin Heidelberg 2009, p. 351-390.

Gold, Benjamin J., *Privacy, Identity and Security*. In Gold Benjamin J. and Lazarus Liora (edited): *Security and Human Rights*. Hart Publishing. Oxford and Portland, Oregon 2007, p. 45-71.

Ministry of the Interior, *Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma)*. (Project on creating personal identities) (Identity Programme) Työryhmän loppuraportti. (Final report of the working group) *Sisäinen turvallisuus*. (Internal Security) Sisäasianministeriön julkaisuja (Publication of the Ministry of the Interior) 32/2010. Helsinki 2010.

Ministry of Justice, *Identiteettivarkaus; henkilöllisyyden luomista koskevan hankkeen (identiteettiohjelma) työryhmän loppuraportin arviointia ja ehdotuksia jatkotoimiksi*. (Identity theft. Assessment of the final report of the working group of the project on creating personal identities, Identity Programme) Oikeusministeriö. (Ministry of Justice). Arviomuistio (Assessment Memorandum) 15.3.2013. OM 4/41/2013. www.om.fi

Monteleone, Shara, *Privacy and Data Protection at the time of Facial Recognition: towards a new right to Digital Identity?* *European Journal of Law and Technology*, Vol. 3, No. 3 (2012).

Nabeth, Thierry, *Identity of Identity*. In Rannenberg Kai, Royer Denis and Deuker André (editors): *The Future of Identity in the Information Society. Challenges and Opportunities*. Springer. Berlin Heidelberg 2009, p. 19-69.

Steinbock Daniel J., *Fourth Amendment Limits on National Identity Cards*. In Strandburg Katherine J. and Stan Raicu Daniela (editors): *Privacy and Technologies of Identity. A Cross-Disciplinary Conversation*. Springer. USA 2006.

²⁰ See the European Commission's Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/22/JHA. Brussels, 30.9.2010. COM (2010) 517 final.

Thomas, Douglas/Loader, Brian D., Introduction. In Thomas Douglas and Loader Brian D. (edited); Cybercrime. Law enforcement, security and surveillance in the information age. Routledge. London and New York 2000., p. 1-13.

UNODC, Comprehensive Study on Cybercrime. Draft. February 2013. United Nations Office on Drugs and Crime. United Nations. New York, 2013.

UNODC, Handbook on Identity-related Crime. United Nations Office on Drugs and Crime. United Nations. New York, 2011.

Van der Meulen, Nicole/Koops, Bert-Jaap, The Challenge of Identity Theft in Multi-level Governance. Towards a co-ordinated action plan for protecting and empowering victims. TILT Law & Technology Working Paper No. 013/2009.

DEMOCRACY, INTERNET AND GOVERNANCE

Fernando Galindo

Professor, University Zaragoza, Department of Penal Law, Philosophy of Law and History of Law
Pedro Cerbuna 12, 50009 Zaragoza ES
cfa@unizar.es; <http://lefis.unizar.es/>

Keywords: *Democratic principles, State of Law, Internet governance, participative democracy*

Abstract: *The paper presents some possibilities to make a democratic use of Internet applying technical and juridical resources that promote an effective putting in practice of the laws and juridical principles of the participative democracy, that are the context of the activities of citizens and institutions according to the principles and rules of the State of Law.*

1. Introduction¹

This paper presents some possibilities to make a democratic use of Internet applying technical and juridical resources that promote an effective put in practice of the juridical principles of the participative democracy, that are the context of the activities of citizens and institutions according to the principles and rules of the State of Law². To that effect, the paper establishes the fundamentals of participative democracy in the State of Law (section 2). In a second step (section 3), the paper presents several examples of indubitable cases of services or applications of Internet and Information and Communication Technologies (ICT), that promote the expansion of democratic uses in the knowledge Societies: our Societies. The next sections (4 and 5) establish some limitations to realize participative democracy as to make political elections by Internet in reason of the existence of: a) some weaknesses related with the technical/political characteristics of the governance of Internet, b) the limits that imposes the existence of the digital divide in broad zones of the population yet, and c) the underdeveloped state of initiatives that the offer of the information/data that the Governments open to the access and reuse of citizens using Internet promotes. The paper presents also (section 6) some possibilities to avoid these limits proposing some examples to overcome the difficulties that the expansion of the participative democracy promotes with respect to the access to and reuse of open data.

¹ The paper is based, partially, on the activities developed in the projects: Ciudad2020, INNPRONTA Project IPT-20111006, funded by the Spanish Centre for Industrial Technological Development, the University of Zaragoza participates in the project as advisor of the Atos Research @ Innovation (ATI) Division of the firm Atos, and Participation in the knowledge society through the activities of the e-Government Observatory. Political, economic and empirical aspects, Project HBP2011-0029, funded by the Spanish-Brazilian ministries of education interuniversity cooperation program.

² As many other authors the paper's position is to attend to the making of the Law from the rules of the Law in the State of Law and of the Soft Law, integrated by proposals that come from another areas: economics, accounting, social sciences, management techniques... as it is the practice in the making of Law and Treaties of the European Union: see in this respect Dawson (2013).

2. Democracy, participation policy and governance

A democratic political system is the one which is organized in response to the guarantee and impulse of three mechanisms, today fundamental legal principles and institutions, recognized in the constitutions and made real in the daily life of the countries where they work.

The mechanisms are those concerning the free election of rulers by the citizens, the effective implementation of the division of the exercise of political power by the relevant agencies, and the safeguard of the protection and promotion³ of human rights by public authorities regarding the activities taking place in the development of the citizens' own lives, of the citizens with businesses as consumers or workers or employees, of companies with each other, of citizens with other citizens, of public administrations with other authorities, of public administrations with companies and vice versa, and of citizens with public administrations and vice versa in relation to the provision of services by the latter⁴.

The three mechanisms are considered characteristic of the operation of the rule of law. Their standard contents and functions are summarized below.

The first mechanism is that of the free election of rulers by the citizens, which is carried out through the implementation of electoral processes that allow for all citizens to participate in government, periodically, by the appointment of their representatives in different political decision areas: state, regional/autonomous or local. This participatory, democratic procedure is supplemented by the possibility for citizens to intervene in government activities through the implementation of another means such as referendum in relation to specific issues subject to the public opinion by political representatives, co-participation in governmental activities through the involvement of individuals or citizens, organizations, civic associations, consumer associations or unions, whose performance is provided in the regulation of administrative procedures, and participation of citizens in resolving legal conflicts by means of their intervention as jurors.

The second democratic mechanism is the separation of powers, that is, the acceptance that the exercise of the resources, tools and methods to be implemented by the elected rulers, must cater to the separation of such exercise into three "powers" or functions: legislative, executive and judicial. This implies that the characteristic activity of each branch must be performed according to the distribution of functional competence established by the procedures recognized and articulated by the constitution and the rest of the legal system. These procedures can ensure both the independence of action of each of the powers, as well as the coordination and balance in the exercise of their characteristic functions or powers.

The third mechanism is the recognition, respect, preservation and promotion of human rights declarations contained in the constitution and the legal system as a whole, carried out by exercising the characteristic powers and functions of the powers with regard to activities taking place in specific societies.

What has been expressed here so far is completed by the view that, obviously, democracy or political participation cannot be implemented effectively in any of the aspects outlined without the satisfaction of a prerequisite: that the citizens are informed or, what is the same thing, have enough knowledge of the purpose of their participation. This knowledge can be, for example, on the characteristics of administrative activities, the effective implementation of the subsidies awarded by the

³ These are ideas commonly accepted in the legal discussion. On the active role of the State in the promotion of rights rather than mere protection, see, e.g., *Carbonell* (2008). See the justification of the approach from the systems theory in: *Nobles, Schiff* (2013).

⁴ Argumentation and communication with respect to concrete problems are in the basis of the praxis of the Law: *Breton, Gauthier* (2011).

Administration in order to satisfy a particular political objective such as providing some schools with Internet access, the political program of a candidate to be elected as a parliamentary member or councilor, the compliance with the political agenda of a political representative who stand for election again, the contents of the decision in a referendum proposal or administrative decision, or the characteristics of a case which the citizen in question has to solve as part of a jury.

That is why today it can be said, in summary, that a democratic political system is one whose operation is based on the informed participation of citizens in the exercise of political power, either indirectly through the election of their representatives, or directly by assisting in making political decisions through other mechanisms. This involves recognizing that citizens can participate, whether by themselves or through their representatives, in virtually all the activities of public authorities, also taking into account the fact that the rule of law today is not the nineteenth-century liberal state that limited the action of public bodies to acting politically as police, developing appropriate basic laws and applying sanctions or penalties to the most serious violators of the legal order: safeguarding the functioning of the market, possible violations, but the State is, at the same time, a social, democratic, welfare, governance State and, these days, the characteristic State of the so-called knowledge or ICT society, which has the power to participate in almost all daily activities, especially those which are characteristic of public institutions since they are publicly funded. We can say also that this State is the State of the participative democracy.

What has been said here so far does not preclude the recognition that the exercise of what is called governance has become accepted as the common political practice of the characteristic powers of governments for some time now. Governance is defined by the Spanish Dictionary as “the art or manner of governing which aims to achieve long-lasting economic, social and institutional development, while promoting a healthy balance between the State, the civil society and economy market”.

This involves recognizing the expansion in the public domain, as characteristic practices or customs of rulers, of the governing principles, techniques or customs which are characteristic of the business environment. This is the same as saying: implementing efficiency and market rules as preferred performance criteria for public authorities.

This action or policy style has to be exercised by the authorities while making it compatible with the implementation of the principles inherent to the rule of law, that summarizes the action of the participative democracy which, by law, governs the action of public authorities, i.e. all those matters on which they are competent according to the legal systems of the State of Law, since they are active agents in the social life of the knowledge society⁵.

To this respect we must add that this kind of policy on governance is compulsory in Spain, for example. The Spanish Constitution was modified (September 2011) to include this policy principle as rule for the activities of the Public Administrations: art. 135 1: “All Public Administrations will conform their actions to the principle of budgetary stability” (“Todas las Administraciones Públicas adecuarán sus actuaciones al principio de estabilidad presupuestaria”).

3. Internet and democracy: real examples

There is no doubt that Information and Communication Technologies (ICT) and the Internet facilitate the operation of democratic political systems and the participative State of Law. Here we present three examples to prove it unequivocally. One is referred to the aids to the election of political representatives. Another one concerns the access of citizens to public services through electronic

⁵ Proposals are made in this regard in relation to the local level in the United States in *Katz* (2010), referred to conciliation between governance and law in *Galindo* (2007). The need of the change of the management techniques in all kind of institutions is presented in *Drucker* (1999)

means. The last one deals with the support to the functioning of the judicial power. The basic characteristics of the examples are summarized in this section.

The first example manifests itself massively mainly in Brazil. Since the second half of the nineties, the electoral processes aimed at the appointment of political representatives are aided by the use of so-called “electronic ballot boxes”.

They are programs and computers that facilitate that voters may exercise the voting rights to elect their political representatives that all citizens have, by selecting the candidates, after authorization by the members of the polling station to voters who are identified through the provision of a document, by pressing the corresponding number, name, assigned to candidates to be elected. The program stores the choices made by voters and adds the final results of the vote.

The results of the votes in each poll station are sent to the Electoral High Court, responsible institution of the organization of the elections. Thus, the use of technological systems improves voting by making it difficult to carry out corrupt electoral practices which in Brazil were allowed by the traditional political election systems based on the use of paper ballot⁶, the use of ICT thereby promoting the broadening and deepening of democracy.

The second example is widespread in many countries. It is the so called electronic government, or more properly, e-government⁷ and, best, e-Administration. It refers to the provision to citizens, through electronic means, of access to public services. It implies that citizens can process on the Internet, from their homes or their own computers, requests to Public Administrations with no need to move to the Public Administration offices from which the satisfaction of a particular right is required: a certificate, a service, a subsidy, a license...

The process takes place as follows. Once the applicant has been reliably identified attending to a security procedure or through a key obtained by using a safe procedure, the interested citizen - the applicant - may submit the application online, along with the record that it is justified or based on, to the computer program of the Administration, electronic office, whose competent administrative section has the obligation to process the file as required by the applicant.

The technological system, ICT, can improve, therefore, the democratic quality of the Administration concerned, by the increasing response readiness of the integrated services, thus enhancing the satisfaction of the rights of citizens⁸.

The third example refers to the judiciary and occurs in several countries⁹.

A lawyer, properly identified, can send a document that is part of a process in which a citizen, defended (or accused) by the lawyer, is involved, to court from any computer, to the effect that the procedural step is considered made, therefore being able to continue processing it in a shorter time than it is necessary for the procedure to go through the established channels for processing a paper

⁶ See, in this respect: *Mezzaroba* (2009).

⁷ The e-government plan of the European Union for the 2011-15 period is regulated in: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, The European eGovernment Action Plan 2011-2015. Harnessing ICT to promote smart, sustainable & innovative Government, COM/2010/0743 final: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0743:FIN:EN:pdf> (25.8.2013). See the reasons of the success of e-government in *Gil García* (2012)

⁸ About online government services for citizens in Spain see: <http://www.060.es/060/appmanager/portal/desktop/page/ciudadanosHome> (25.8.2013).

⁹ The operation of the Spanish system LEXNET is taken as a reference: “Lexnet telecommunications computer system for submission of papers and documents, transfer of copies and performing procedural acts of communication by electronic means”, regulated by Royal Decree 84/2007, of 26 January. Information on the LEXNET system can be found in: <https://www.administraciondejusticia.gob.es>. A detailed study on the implications of the use of Information and Communication Technologies for the jurists in Spain is in: *González de la Garza* (2012). On e-Justice in the European Union see: *Oliva, Gascón, Aguilera* (2012)

document, by avoiding delays which are characteristic of the operation of ordinary mail. The system also allows all parties involved in the process to check the status of the procedure, making it possible to know both the completed phases of the process and the content of the documents submitted by the other party or any decisions or measures taken by the prosecuting or judging body.

ICT in this case also promote to shorten the time required for the characteristic work of judicial power: conflict resolution, and also makes the phases of the procedure more transparent, while allowing the parties involved to know the status in which the processing is, without thereby the judicial losing process functions conferred upon it by the democratic system.

There is no doubt that these processes are examples of how ICT are effective tools to support the functioning of democratic systems.

4. Internet as enhancement of communication and promotional tool of the participative democracy

In order to explore other possibilities, completing the most significant theories and cases of democracy expressed in sections 2 and 3, we reason in the rest of the paper on how ICTs can improve the participation of citizens in implementing the rule of law by allowing them to intervene in policy decisions with a broader and better knowledge of political reality and functions than they have without the use of ICTs. We shall see, at the same time, that the promotion of participative democracy of ICT is different to the affirmation that “Internet is the same as democracy”.

4.1. Democracy and Internet

The term democracy appears repeatedly on the Internet. And this is not only regarding the accumulation of substantive information, of contents, i.e. Definitions, terms, theories and concepts, that are made on Internet about democracy, where it is understood as a term which helps to characterize those political regimes in which citizens elect their representatives and thus participate in the process of public governance, but also in regard to the relationship, often the equalization, between the Internet and democracy. These statements understand that the functioning of the Internet or the “net” is democratic, or conducive to democracy, considering that it provides to all those who manage it, those who ultimately have a means of access to it: computer, mobile phone or (interactive) TV, for example, with some knowledge/power/control over the reality that they did not have before. The access to information was reserved for those who had been appointed “rulers” in the process of electing political representatives democratically, but the Internet brings the possibility to inform to all their users.

In these pages, we discourse about these issues by focusing in particular on the second aspect, contrasting it with the first, i.e.: finding out the effective strengthening of democracy, understood as political participation, generated by the use of the Internet.

We provide to that end some thoughts on the fact that access to the Internet, and through it access to information, does not involve an increase in political participation but in communication (in this section, 4.2). We look also the relevance of the so called digital divide as a barrier to a hypothetical exercise of participatory democracy by citizens using the Internet (section 5). We pay finally attention to certain initiatives that enhance the effective realization of democracy through the use of the Internet, assuming that democracy is also the participation of well-informed citizens in public activity (section 6) .

4.2. Internet as access to communication

At the beginning of this paper we stated that a prerequisite for the exercise of democracy is to have enough information to decide. This is consistent with the fact that no decision¹⁰ can be taken without information. If this is true of people's own activities: in the exercise of freedom or the principle of autonomy of the will, it refers more relevant in the scope of human action to activities involving other persons. Also in political action and the democratic exercise of free election of political representatives: it is not possible to elect without prior knowledge of the options that may be eligible.

And the Internet provides, without doubt, access to information¹¹. It offers information that did not use to be available to the citizens without it. Information was, at best, collected in documents: studies, reports, scientific papers and opinion articles, books and news provided by means of publication, opinion and information: newspapers, magazines and other media (mainly television and radio). Another part of information, and especially that concerning the activities of the State was outside the circles of opinion. Quite often it was considered secret: it was available only to State institutions, their civil servants or the representatives of the citizens in the Parliament.

The information needed in order to elect democratically is that related to the activities of political representatives, whose expression is manifested in the characteristic action of the institutions in which they perform them. They are the activities of the legislative, executive and judicial powers. They are contained in laws, rules, regulations, sentences, and now also in web pages which present both the content of the regulations and information about the features and results of the activities performed and public services offered by each institution (open data).

The information about the contents of the regulations is the same, in digital format, as that which was made public on paper. The main difference results from the spreading degree of digital information: it is greater than that collected in paper format. Information on the institutions, their activities and services, is of a different nature: previously it did not use to be accessible, or at most there was some echo in the media. In most cases it was expressed in the content of legal texts or regulations themselves. Currently this information is generated by the institution itself, which may offer its services to citizens via the Internet, as we mentioned above (section 2, ICT and democracy).

This information needs to be exposed, advertised and collected in an orderly and clear enough way if one wants to enable citizens to access it, to use public services and to perform the democratic control of it which is the responsibility of the citizens. Some guidelines must also be established for the proper realization of this collection, based both on the content of the practices performed and on what is prescribed by the rules of democracy aimed at enhancing the participation of citizens in political power. Initiatives aimed at conveying the public information which can be found on the Internet¹² to citizens deal with all this.

¹⁰ Without establishing contacts with the outside world. See in this regard *Maturana* (2006). This article shows the origin of self-consciousness, showing it as a case that occurs in "language", and not confusing the domains in which life occurs, or reducing them. For this he is based on biological and cultural foundations of what is human, always seeking the structural-operational mechanism that gives rise to the phenomenon by which asking occurs without introducing semantic notions. The author also reflects on the impact and scope of this look, that is, self-consciousness does not occur in the brain and is not a physical entity but is occurring as a configuration of feelings (sensory) in a continually changing present.

¹¹ With problems with the used access programmes as Google, see: *Reischl* (2008)

¹² There are several catalogues of public administrative data collected by various government institutions. Prepared by the Government of the Basque Country: <http://opendata.euskadi.net/w79-home/es> (25.8.2013). On administrative activities of the Government of the United Kingdom: <http://data.gov.uk/> (25.8.2013). On USA initiatives: <http://www.data.gov/> (25.8.2013). On Spanish initiatives: <http://datos.gob.es/> (25.8.2013). With respect to Brazil see: <http://dados.gov.br/> (25.8.2013). The Open Data Foundation, a non-profit organization, promotes the use of statistical data: <http://www.opendatafoundation.org/> (25.8.2013).

Any observation of the information collected by this type of initiative realizes that it responds to diverse goals or objectives: the offer of information to those who carry out studies, to have secure access to public services, to show the extent of administrative initiatives characteristic of the administrative body that is responsible for the web page or site, to denote the progress of technology, to implement the legal principle of transparency in government activities, to show the efficiency of governance policies, to generate activities to be undertaken by businesses and thereby create employment... All of which brings about the existence of a wealth of information on the Internet, still barely accessible to the citizens, since they do not have sufficient knowledge or resources to be able to access the information and, once accessed, to understand it. This, therefore, is not only due to the limited number of people accessing the net, the digital divide, but to the fact that information is frequently placed with the language that is characteristic of professionals with an expertise in accounting, for example, but not in language understandable by the citizens. This is that the resources of the Internet do not facilitate the fundamentals of the political communication but, in many occasions, the pure communication or propaganda of the own activities or the emissary, of public or private character.

5. Digital divide and Internet governance as obstacles to participative democracy

At the beginning of the last section (4.1) it has been outlined that the term democracy is very often used as a term that characterizes the Internet. It is said to promote participation. This is to show to the public opinion, the citizens, information that was previously only held by government bodies or political parties, to allow everybody to express opinions about some issues presented on the net by Governments, individuals, associations or companies. We have seen that this is not participative democracy, it is only participating in the communication or propaganda of the own activities (section 4.2), because they are the purposes of the publication of the information.

In this section we present another limit that may be established such claims. In particular we focus on:

Showing the basic characteristics of the uses made on the Internet at the moment, checking whether the claims made about the possible effective promotion of democracy are justified, understood as an expression of political opinions by citizens, by the mere existence and use of Internet applications or programs,

Outlining some of the features of Internet governance, especially as regards the possibility to express opinions freely and secretly, a characteristic function of democracy in the Rule of Law, which is actuated by participating in the election of political representatives, in order to ascertain to what extent the operation of the Internet allows the setting in motion of this type of activity, and

Putting as reference the boundaries to access to the content of the information stored in the Internet.

5.1. Internet use and promotion of democracy

For the purposes of considering specific data, we look at information related to Internet use in two areas: percentage of homes or households with Internet access and of individuals that use regularly Internet, and percentage of declared uses of Internet applications.

5.1.1. Homes and individuals

There is no point in denying the high level of Internet access that occurs at the moment. Attending to official statistics (EUROSTAT)¹³, they state that the average number of households with Internet access in Europe in 2012 is 76 percent, compared to 55 per cent in 2007¹⁴. The amount is adequate. The percentage of users are reduced slightly if we consider that the number of individuals that uses the Internet regularly is in 2012 in Europe 74 percent. Anyway both numbers are acceptable.

5.1.2. Applications used

There are also statistics on the type of applications, programs or uses made on the Internet. According to these data, the Internet is used primarily to perform the following types of communications:

- 1) Individuals using the Internet for finding information about goods and services, they are in Europe in 2012 the 61 percent of the users;
- 2) Individuals using the Internet for participating in social networks, they are in Europe in 2011 the 38 percent of the users, and
- 3) Individuals using the Internet for posting messages to social media sites or instant messaging, they are in Europe in 2012 the 40 percent of the users.

It is reasonable to consider that when we deal with democracy only communication referred in the second and third place, using the Internet for participating in social networks or for posting messages to social media sites, can be taken as a reference to discourse on a possible exercise of democracy by using the Internet. Let us remember that, as we saw in the first section (Democracy, participation policy and governance), democracy is the same as issuing opinions with public relevance or “participation of citizens in the exercise of political power, either indirectly through the election of their representatives, or directly by assisting in making political decisions through other mechanisms”. The use of the Internet for finding information about goods and services is some different to practice democracy.

Returning to the statistics, it is interesting to note, looking at the figures compiled for Internet use in Europe, that the use of the Internet for finding information about goods and services in 2012 is the most widely used medium by all users regardless of their age. Specifically, 74 percent of the users between 16 and 24 use it, 71 percent of the users who are between 25 and 54 do, and 38 percent is the percentage of users who are aged between 55 and 74 who use it. The percentage of users who use the Internet in 2012 for posting messages to social media sites or instant messaging are lower in general (40 percent), but have these differences: 81 (between 16 and 24 years of age), 44 (between 25 and 54) and 12 (between 55 and 74). The percentage of users who use the Internet in 2011 for participating in social networks are similar in general (38 percent) to the percentage of users who use the Internet in 2012 for posting messages to social media sites or instant messaging; there are differences of percentage attending to the age: 80 (from 16 to 24 years of age), 41 (between 25 and 54) and 11 (between 55 and 74).

5.1.3. Conclusions on the use of the Internet and democracy

The data presented here so far allow us to conclude the following.

While the Internet has undoubtedly achieved a strong growth, the average network access is 76 percent of European households in 2012, it does not allow, hypothetically, for example, the adoption of

¹³ <http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home> (25.8.2013).

¹⁴ The figure regarding households with an Internet connection appears to be the most significant one in relation to those used by statistics: the one about individuals who use the Internet is too generic.

a Europe-wide standard establishing the obligation to elect political representatives by using ICTs: from the people's own computers. For this rule to come into force such access should be guaranteed to hundred percent of the population, which does not occur today.

The expansion of democracy is not quite viable right now if we take into account the characteristics of Internet users. As we have seen, only the youngest sector of the population: the one between 16 and 24 years of age, uses systems that make it possible to express opinions (80 per cent of them attending to general European figures), while the other two sectors between 25 and 54 and between 55 and 74 uses them to a limited extent (44-41 and 12-11 percent respectively).

5.2. Internet governance

There is another problem of greater importance than that of the small number of users accustomed to using the net to issue opinions that we have just noted as a limit to the expansion of democracy on the Internet^{15 16}. We identify this problem as Internet governance.

By Internet governance, we refer to the basic rules of operation of the system which, beyond the use of technologies, come to be, with some qualifications, the same as those of the market or profit making.

Indeed. The use of the Internet requires, inevitably, that the citizens pay for its use: primarily to the telecommunications company that ensures communication and to the provider of Internet access service that makes "surfing" possible, also to those who offer "accessible" services through the net. The last payment is made in an indirect way: either by paying the price of goods acquired, once the costs of marketing and shipping the product incurred by the seller by using the Internet have been passed onto that price or, in the case of access to public services, by paying taxes and fees to the State, as part of them are used to cover the cost of the services that are accessible and processed online¹⁷.

To this must be added another facet or dimension if we consider the hypothesis of the Internet as a channel for exercising democracy in the process of electing rulers or through the issuance of opinions in a referendum on an issue subjected to the decision of citizens by public institutions. The new dimension comes from the fact that although, as already seen in the examples mentioned above (ICT and democracy) relating to access to services of public administration or the processing of court cases, the exercise of such access required unequivocal identification of the person issuing the opinion, just as in the application for public services or acting in the administration of justice: it must be known who are exercising their rights and that they are doing so at a particular time, while the performance of democracy through elections, however, requires something else: to guarantee and preserve the confidentiality of the opinions to the effect that these are made freely (voting requirements are: universal, free, equal, direct and secret suffrage). And it is here that the relationship between democracy and the Internet has so many difficulties that it can be even said that right now such relationship is not possible, even counting on technological resources or means of payment as emphasized below.

¹⁵ The size of the problem is smaller due to the fact that the number of users accustomed to voicing their opinions on specific issues on the net is likely to increase in the coming years as generational change occurs. The larger problem is linked to the performance characteristics of the Internet and its regulation, preventing to guarantee the secrecy of the issued opinions, a principle which, inter alia, is required by the implementation of democratic processes.

¹⁶ Let us remember that these systems require a universal, free, equal, direct and secret suffrage.

¹⁷ It is necessary to incur these expenses because those who offer products or services, whether they be companies or the Administration, also have costs: they must be incurred both in terms of the costs that are specific to the development and marketing of their offer in a medium like the Internet, as well as in terms of the cost to be borne in order to provide products or services on a website that has an Internet address or domain, whose implementation and maintenance requires both paying the domain name provider for the costs of the domain as well as the costs borne in order to keep communications, computers and programs required by the publication of a website on the Internet.

Both the electronic procurement of public services as well as submitting documents to the courts requires ensuring the authenticity of the sender, that of the communication process or the submission of documents: it may not be intercepted, and the content of what is sent must be what was actually sent by the sender, which happens through the use of the technical requirements set out briefly above, but these procedures do not require permanently keeping the content of communication secret. Moreover, in the processing of administrative and judicial procedures, it is necessary, basically, to be able to prove throughout the entire procedure that the contents of the documents provided are endorsed by the sender.

The fundamental requirement to ensure the functioning of the process of issuing a political option or opinion, however, as established by democratic systems, is the permanent preservation of the secrecy of the option or opinion of the person who is responsible for it, otherwise voters or those expressing opinions may not have sufficient freedom to cast their vote or option, another basic principle of democracy. The problem lies in the fact that, although reliable identification is possible, as in the examples mentioned in section two, by using ICT identification systems with higher or lower costs, ensuring the preservation of confidentiality and freely issuing views cannot be put into practice but, at most, by using mechanisms such as public key encryption for confidentiality, whose general use is not authorized at this time for security reasons.

That is: in the case of Internet voting, the principle of public security establishes strong limits on the principle of market or governance rules governing the characteristic operation of the Internet, and which is what defines right now, basically, the practice regarding the free expression of ideas that occurs between Internet users through the use of communication tools such as access to social networks, sending news to “blogs” or exchanging messages through electronic mail systems, telephone communication and video conferencing.

5.3. Use of technical tools and digital divide

We come back to remember here that one relevant prerequisite for the exercise of democracy is to have enough information to decide. This is the same to say that it is not possible to elect or select without prior knowledge of the options that may be eligible.

The internet gives communication or, in any cases, propaganda. It provides access to information collected in documents: studies, reports, scientific papers and opinion articles, provided by newspapers, magazines and other media. But another part of information, and especially that concerning the activities of the State was outside the circles of opinion. It was available only to State institutions. Currently this information begins to be generated by the institutions, which may offer their services to citizens via the open data/open government initiative by Internet.

The problem is that the citizens do not have sufficient knowledge or resources to be able to access this information and, once accessed, to understand it. This, therefore, is not only due to the limited number of people accessing the net, the digital divide, but to the fact that information is frequently placed using the language that is characteristic of professionals with expertise in accounting, for example, but not in language understandable by the citizens.

It is appropriate to reconsider the information provided by statistical data in order to have greater awareness of the possibilities and implications of a hypothetical attempt to perform an exercise of democracy, understood as the exercise of political suffrage, participative democracy, by using the tools and mechanisms provided by the Internet.

In the previous section we noted that political elections are not possible through the Internet because the technical instruments which would, apparently, make them possible have not even been developed for the use of the tools required for this is not allowed. We have also found that the statistics concerning the use of the Internet state that, while in Europe there are a good number of peo-

ple who access the Internet, the number of those who express their views through the net is not so large: they express their views in closed circles, social networks, or public writings. We saw that only the young people reported often using applications or programs that allow the issuance of such opinions. In this section we are going to further refine the scope of these arguments, showing that when we move from considering the general statistical averages related to a broad spectrum of people to observing those relating to individual countries, and even regions within individual countries, the figures have different contents and meaning.

Let us look at the figures relating to the percentage of households with Internet access. We said that the average access in Europe was high: 76 percent of homes had it in 2012. The numbers have a different shape if we look at Spain, where the percentage is 68, Germany, 85 or Romania, 54, for example. The tint is even more important if we look at South America. In Brazil, in 2012, only 40 percent of homes had Internet access, with the same average number being 44 per cent for households located in urban areas and 10% of the homes located in rural areas¹⁸.

These data account for the reality of the actual existence of the so called digital divide and how the reflection on the possibility of voting or participating in the political arena via the Internet is a narrow discourse. This has a limited immediate social scope, it needs to be completed. Let us consider that a hypothetical immediate implementation that would require mandatory use in a country would imply depriving huge numbers of people¹⁹ for two reasons: the digital divide and the fact that the information to decide is not adequately accessible.

6. Participative democracy by Internet, two examples: digital inclusion of maps and smart cities

There are initiatives for some time now that aim to promote the active participation of citizens in the exercise of their democratic rights, by making the Internet accessible to the citizens, not only to the data/ information/propaganda generated by governments but also to the operation and activities themselves of public Administrations and the various public powers²⁰. To this end several approaches and technological resources are used that place greater emphasis on the promotion of democratic participation and digital inclusion than on the implementation of the technological development itself through e-democracy, which is dealt by another different kind of research²¹ in the boundaries that we have exposed before (sections 4 and 5).

The first initiative is oriented to indicate by the design of knowledge maps the grade of participative democracy that several government initiatives directed to offer transparency by web portals promote. The second initiative studies the fulfillment of the basic democratic juridical principles by several offers of services to citizens based on the use of open data that are elaborated in relation to the design of smart cities.

¹⁸ See the statistical date on Brasil in: <http://www.cetic.br/pesquisas-indicadores.htm> (25.8.2013).

¹⁹ But there is room for discussion because, in spite of what has been said, there is no doubt that, at least in theory, technical tools exist so that this can be done. Another thing is what happens in reality: the techniques are not as generally implemented as to ensure that all citizens can use them nor, on the other hand, the users who are fluent in their use, and therefore can participate, are representative of the views present in a particular place. The figures indicate that this is so: only the young people move with ease in the digital arena. Their views represent a part of society. The percentages of users make reference to specific bands of the population and not others: age reasons, but also those concerning training and education, are behind the limited use of the Internet in relation to large numbers.

²⁰ European transparency directive: Directive 2003/98/EC of the European Parliament and Council of 17 November 2003 on the reuse of public sector information. Art. 1.1: "This Directive establishes a minimum set of rules governing the reuse and practical tools to facilitate the reuse of existing documents held by public sector bodies of Member States". <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:EN:PDF> (25.8.2013).

²¹ For example: <http://forums.e-democracy.org/> (25.8.2013).

6.1. Maps for the citizens

Research and developments carried out by the International Observatory on e-government since 2003 fall within this framework.

The main objective of the EGOBS (Electronic Government Observatory) Observatory is the independent study of the characteristics of the accomplishments in the field of e-government, that is the set of organizations and systems which are needed in order to produce the provision of administrative services to citizens and companies by the Public Administrations with the help of resources provided by Information and Communication Technologies, taking place in different countries.

The papers were put special emphasis on checking whether the provision referred to is made with respect to the rules, procedures and principles enshrined in laws, including the right of citizens, companies and institutions to participate in such activities and, especially if the regulations on data protection and security of electronic communications are met in its implementation.

EGOBS (www.egobs.org) is an initiative arising from the E-Government thematic network coordinated by the University of Zaragoza (Spain) and in whose activities have been involved since 2003 the Universities of Burgos and Valladolid (Spain), the University of Münster (Germany) and Queen's University of Belfast (United Kingdom), on the European side. American members are the National University of La Plata (Argentina), Diego Portales University of Santiago de Chile, the University of Havana (Cuba) and República University of Montevideo (Uruguay). The Association for the Promotion of Information Technology and Electronic Commerce (APTICE) contributed to the activities of the Observatory. The Observatory is part of the Legal Framework for Information Society, LEFIS.

Since 1 January 2009 the Observatory has had staff and equipment infrastructure to develop its activities in Latin America. Specifically, in the Federal University of Santa Catalina (Brazil)²².

EGOBS's monitoring activities have been focused on applying, for teaching and research purposes, a methodology developed to study websites made and implemented by public authorities, by using analysis criteria which enable understanding and publicly presenting the characteristics of the pages themselves, their content and those of service offerings performed by the Administrations that have made and maintained²³ them.

The methodology has been applied since 2005 to web sites developed by public institutions in Chile, Uruguay, Spain and Brazil, mainly. The results of the analysis are exposed on the Internet.

Since 2009 EGOBS has been performing another type of analysis on the same line aimed at providing citizens, on the Internet and clearly, with the geographic location of public institutions that perform various activities. This information refers mainly to Brazilian institutions.

Studies are in the form of web pages containing maps of Brazil in which the location of institutions and activities undertaken by them in relation to specific matters²⁴ are recorded.

The list of materials in the form of general topics is currently the following: the environment, culture and public education, democracy, convergence and digital inclusion, public finance, the judiciary, the prosecution, e-government models and projects, public health and public security. Fundamental used general categories are related with the articulated attending to the principle of separation of powers: legislative, executive and judicial.

²² <http://www.egov.ufsc.br/portal/> (25.8.2013).

²³ LEFIS metrics. View its content in: http://www.egobs.org/index.php?option=com_content&task=view&id=14&Itemid=27 (25.8.2013).

²⁴ See the maps in: http://www.egov.ufsc.br/portal/projeto_mapas (25.8.2013).

In relation to each topic, several maps are shown on federal or state scales, which locate, for example, the position of institutions, research centers, activities carried out, distribution of public resources with respect to specific projects, web sites analyzed following the LEFIS methodology.

The maps are the result of research conducted under the responsibility of individual or group of researchers who prepare papers or articles on the respective area. They are intended to create discussion while, primarily, showing the subjects studied to citizens who have no specialized training, but are simply interested in learning about specific issues in order to create political opinion. In this sense, they are technological tools that promote democracy²⁵.

New researches like to develop updated criteria to characterize the grade of democracy of the analyzed portals.

6.2. Smart Cities

The internet lets to promote today information/communication/propaganda put by the firms/institutions/governments/social networks/physic persons that like to make public this kind of information. The internet lets to use, also, basic information in the form of data that are captured by adequate sensors in the things/ movements of the nature or are generated by citizens, governments, firms or social network's activities. They are the open data that can be reused or utilized in other services and programs or applications.

The technological development lets build these applications, and the Laws promote the put in practice²⁶.

A broad extended instrument to make reality these wishes is the construction of smart cities, this is services or applications that require such date to build services for a sustainable growing according with ecologic and democratic principles and rules. These services are reusable by other consumers or citizens based on the making of several contracts between the misuse of information, the providers of information or data, the users of services, the firms creators of services and the authorities that make public the general information using their resources. These activities foment the realization of private-public joint activities that fulfill the objectives established by the Laws and principles of the State of Law.

One of these projects is the City 2020/Ciudad 2020 (2011-2014)²⁷.

The project is integrated by these partners:

Companies: INDRA (informatics), FAGOR (electrodomestics), FERROVIAL (highways), ATOS (engineering), GFI (informatics) and small businesses (informatics).

Universities (subcontracted partners): Polytechnic of Madrid, Carlos III, Santander, Coruña and Zaragoza.

The project is acknowledged and funded by the Spanish Program INNPRONTA.

²⁵ On the fundamentals of the maps: *Rover* (2013)

²⁶ Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:345:0090:0096:EN:PDF> (25.8.2013). Spanish Law 37/2007 of 16 November on the re-use of information of public sector: <http://www.boe.es/boe/dias/2007/11/17/pdfs/A47160-47165.pdf> (25.8.2013). Spanish Royal Decree by which develops the law on re-use of the information of the public sector, to the State public sector, approved in Council of Ministers 21.10.2011: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-17560 (25.8.2013). Draft law of transparency, access to public information and good governance. Under discussion in the Spanish Parliament.

²⁷ See the most relevant information on the project in: <http://www.innprontaciudad2020.es/index.php/en> (25.8.2013)

The most important objectives of the project are to build services for the citizen with the possibilities offered by ICTs attending to the technological resources of the “Internet of things” and Smart Cities. In the following areas:

Activities carried out in the interior of buildings: control of the energy consumed, for example.

Activities on trips using public or private vehicles: establishment of routes attending to past experiences and the state of the traffic of vehicles.

Activities developed in order to implement initiatives of sport or tourist nature: proposals of adequate routes to walk, tourist destinies.

Activities developed with the purpose of enforcing administrative rights.

The implied legal principles that are respected in the design of the project City 2.020 are, in summarized form²⁸ these:

Protection of personal data and use of anonymization processes with respect to the use of personal data.

Preservation of intellectual and industrial properties.

Liability: responsibility of the services and the capture of information.

Satisfaction of legality with regard to the processes of gathering information, modelling (‘data/reality mining’) and building of programs with respect to the re-use of:

Public open data

Open private data:

Generated by other companies.

Generated by 2.020 city services.

7. Conclusion

Those stated in this paper are different, specific ways to create democracy via the Internet and thus are different possibilities to enhance democracy. The alternatives show that, although democracy on the Internet will always be limited by the inevitable “interested” intervention of the Internet governance, there is room for increasing democracy, understood as citizen participation in the knowledge of public activities, while simultaneously enabling digital inclusion by using the resources contained on the Internet. These are the reasons why the exposed are different, concrete forms, to create democracy via the Internet and therefore different possibilities of increasing real democracy. Possibilities show that if democracy on the Internet will be limited by inevitably operation of Internet governance, there is scope to increase it, if we understand it as citizen participation in knowledge of public activities, and promotion of digital inclusion using the resources that the Internet provides.

8. References

Breton, Philippe, Gauthier, Gilles, Histoire des theories de l’argumentation, la Découverte, Paris, pp. 3-7 (2001).

Carbonell, Miguel, Constitution’s functionality and social rights: outline of some problems. In: Estudios Constitucionales, Vol. 6/2, pp. 43-71 (2008).

²⁸ The information is given as example. The project is in development today and it is convenient to wait for the final results to make a more juridical description of the services that the Programme will offer.

- Dawson, Mark*, Soft Law and the Rule of law in the European Union: Revision or Redundancy?. In: Vauchez, Antoni, De Witte, Bruno, *Lawyering Europe. European Law as a transnational social field*, Hart Publishing, Oxford, pp. 221-241 (2013)
- Drucker, Peter F.*, *Management Challenges for the 21st Century*, Harper Collings, New York, pp. 2-40 (1999).
- Galindo, Fernando*, Justicia, gobernanza y legalidad. In: *Seqüencia*, Vol. 55, pp. 29-64 (2007).
- Gil García, J. Ramón*, *Enacting Electronic Government Success*. Springer, New York, pp. 137-178 (2012).
- González de la Garza, Luis, M.*, *Justicia electrónica y garantías constitucionales*, Wolters Kluwer, Las Rozas, 705 pp. (2012)
- Katz, Ellen D.*, Engineering the Endgame. In: *Michigan Law Review*, Vol. 109/3, pp. 349-386 (2010).
- Maturana, Humberto*, Self-consciousness: How? When? Where?. In: *Constructivist Foundations*, Vol. 1, issue 3, pp. 91-102 (2006).
- Mezzaroba, Orides, Rover, Aires, J.*, A urna eletrônica: sua contribuição para o aperfeiçoamento da democracia representativa partidária brasileira. In: Galindo, F., Rover A.J., (Eds.), *Derecho, gobernanza y tecnologías de la información en la sociedad del conocimiento*, LEFIS Series Vol. 7, Prensas Universitarias, Zaragoza, pp. 63-73 (2009).
- Nobles, Richard, Schiff, David*, *Observing Law through Systems Theory*, Hart Publishing, Oxford, pp. 164-206 (2013).
- Oliva, Andrés, Gascón, Fernando, Aguilera, Marien*, (Eds.), *La e-Justicia en la Unión Europea*, Aranzadi, Cizur Menor, 279 pp. (2012).
- Reischl, Gerald*, *El engaño Google, Medialive Content*, Barcelona, 192 pp. (2008)
- Rover, Aires, J.*, Observatorio do Governo Eletrônico e conteúdos geoprocessados. In: Galindo, F., (Ed.), *El derecho de la sociedade em red*, LEFIS Series Vol. 14, Prensas Universitarias, Zaragoza, pp. 21-39 (2013).

INFORMATION RIGHTS AND OTHER FUNDAMENTAL RIGHTS: DYNAMIC INTERACTION IN THE CHANGED ASYLUM SYSTEM

Terhi Anttinen

Research assistant, NETSO (Network Society as a Paradigm for Legal and Societal Thinking);
Project director: Professor Ahti Saarenpää, Institute for Law and Informatics, University of Lapland
P.O. Box 122, FI-96101 Rovaniemi Finland
terhi.anttinen@ulapland.fi

Keywords: *Legal Informatics, EU asylum law, information rights, fundamental rights*

Abstract: *The paper is part of my work as a research assistant and leads into a future study in which I hope to create a theory about the dynamic interaction of fundamental rights. The theory differs from the balancing of fundamental rights, in which fundamental rights are realised “more or less”. In negative dynamic interaction, the success of one right can be dependent on that of another right. (If right x is not realised, neither is right y.) In positive dynamic interaction the success of one right makes it more likely that another will succeed as well. (When right x is realised, so is right y.) The dynamic interaction of fundamental rights is highlighted in asylum cases in the European Union, an area of law where information rights play a significant role. It is thus also a fruitful context for the study of how information rights in particular interact with other fundamental rights. One aim of the theory is to inform a method, or at least a practical tool that would describe and explain the application and realisation of fundamental rights with an appropriately critical approach to information and communication. This would offer a corrective of sorts where the present realisation of fundamental rights is concerned.*

1. Changes in the legal system that have affected asylum law

National legal systems have been in a state of rapid change in recent decades. As Aulis Aarnio has written, jurisprudence participates in systemic changes by parsing concepts and refining the relationships between them¹. In the same vein, Ahti Saarenpää has noted that the legal system is changing and it must change if we are to successfully identify and re-evaluate problems. He continues that we have not always woken up to changes in time². The application of European Union law (EU law) is one of the changes that have posed new challenges for national authorities. For example, Tuomas Pöysti has pointed out how EU law now appears as a distinct layer of law that covers more and more fields of legal life and that has to be applied in judicial operations in accordance with its rules³. Increased European cooperation also requires common information management systems. For example, in the case of asylum seekers, significant amounts of sensitive personal information are collected in the Eurodac database⁴. This information makes it possible to monitor whether asy-

¹ Aarnio Aulis Tulkinnan taito: ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. WSOY, Helsinki (2006).

² Saarenpää Ahti Kadonneet systeemit. Werner Söderström lakitieto, Helsinki, 272 -273 (1997).

³ Tuoman Pöysti Tehokkuus, informaatio ja eurooppalainen oikeusalue, Helsingin yliopisto, Yliopistopaino, 530 (1999).

⁴ Regulation (EC) No 2725/2000 Article 1.

lum seekers move from one member state to another. According the Dublin II Regulation, an asylum seeker can be returned to the member state which he or she first entered⁵. This paper illustrates how changes in the asylum system highlight the role of databases and how individuals' right to get information figures prominently in the digital environment. The paper also emphasises the importance in the new legal operational environment of high quality in legal information and legal knowledge and of successful communication during asylum procedures.

Johanna Tornberg has stated that the legal framework includes a number of information processes that comprise information processes of their own.⁶ Also the asylum system of EU composes of a number of information processes. The procedure whereby the EU and Schengen countries identify the member state responsible for examining an asylum application can be described as an information procedure, and merely in this procedure is detected several information processes. The member states co-operate mostly through the information infrastructure known as DubliNet⁷. The European Union's Common Asylum System (CEAS) consists of judicial, sensitive, informative and technical information. However, the system has not worked appropriately. A number of high-level agencies and human rights organizations have become aware of serious weaknesses in the CEAS. Reports have often cited shortcomings in Italy, Malta, and Greece⁸, but there appear to be serious problems in other countries as well⁹. In reality, some member states cannot offer the material reception conditions or fair asylum procedure required by EU law. This has exposed asylum seekers to different kinds of violations and many have been forced to flee to some other state.

Despite the violations noted, the authorities of member states have returned several asylum seekers to what were inhuman and degrading reception conditions. These Dublin returns are justified by the legal interpretation of the Dublin II Regulation and are based on the registry entries of Eurodac. For example, in 2012 the Finnish Immigration Service presented Italy with 122 requests to take charge of and 71 requests to take back¹⁰ asylum seekers. In 2011, the corresponding figures, again for Italy, were 120 and 77. Finland sent 62 requests to Malta to take back asylum seekers¹¹. In addition, before the European Court of Human Rights (ECtHR) rejected the return of an applicant to Greece in *M.S.S v. Belgium and Greece* in 2011¹², Finland presented Greece with several requests. However, member states have the discretion to examine an asylum application contrary to the criteria laid down in the DublinII Regulation. In fact, according to EU law, a member state is required to take responsibility for the examination if a Dublin return would infringe an asylum seeker's rights as safeguarded in the Charter of Fundamental Rights (CFREU). The Court of Justice of the European Union (CJEU) confirmed this in a judgment in 2011¹³.

The Finnish Ombudsman for Minorities, Eva Biaudet, examined fifteen Dublin returns from Finland to Greece or Italy during the period 1.1 - 31.8.2009. All the asylum seekers were either women under 35 years of age or minor girls and boys. In most cases, the applicants had suffered sexual

⁵ Regulation (EC) No 343/2003.

⁶ Tornberg, Johanna, Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu. Lapin yliopistokustannus, Rovaniemi, 98-100 (2012).

⁷ See e.g. *Eurodac Supervision Coordination Group: Recommendations on the use of DubliNet* (2010).

⁸ See e.g. *Pro Asyl The Living Conditions of Refugees in Italy*, A Report by Maria Bethke & Dominik Bender. Report on the research trip to Rome and Turin in October 2010 (2011), *Amnesty International Seeking safety, finding fear: Refugees, asylum-seekers and migrants in Libya and Malta* (2010), and *Amnesty International: The Dublin II trap, transfers of asylum-seekers to Greece* (2010).

⁹ See e.g. *United Nations High Commissioner for Refugees Regional Representation for Central Europe, Refugee Homelessness in Hungary*. Budapest, Hungary (2010) and *Irish Refugee Council/ NGO Forum on Direct Provision Direct Provision and Dispersal: Is there an alternative?* (2011).

¹⁰ For more details, see (EC) No 343/2003, chapter V "Taking charge and taking back".

¹¹ *Maahanmuuttovirasto, Turvapaikkayksikön tilastokatsaus 2011 and 2012*.

¹² Case of *M.S.S. v. Belgium and Greece* 30696/09, 21.1.2011.

¹³ In Joined Cases C-411/10 and C-493/10, Court of Justice of the European Union, 21.12. 2011.

abuse, other violence or political persecution in their home country. In almost every case, they encountered physical and/or sexual violence in Italy or Greece as well. The violence was mostly perpetrated by officials or by others who had officials' approval. Biaudet noted that violence was also an indirect consequence of the lack of proper reception conditions. She also remarked that in more than half of the cases clear signs of human trafficking could be clearly seen from the documents. In any event, because the applicants had already been registered in Eurodac in Greece or Italy, a deportation decision was issued without any individual examination - even though the Italian authorities had requested that the deportation of vulnerable persons to Italy should be limited in some cases¹⁴.

As the above shows, the authorities do not always wake up in time to changes in a system. The data recorded in Eurodac has been used detached from its surrounding legal system and the applicants do not always receive sufficient information about their rights in connection with the application of the system. Moreover, communication between the authorities may fail. Yet, the changes made in the system were not designed to break the coherence of the earlier system: authorities cannot infringe an individual's fundamental rights "legally" by Dublin returns. The Eurodac data system has been created exclusively for the application of the Dublin system. However, the Finnish authorities have ignored inhuman and degrading reception conditions, exposing the applicants to situations in which they might once again fall victim to human trafficking.

Similar issues have frequently been discussed in research on legal informatics. Legal informatics is intrinsically linked to changes in society and the constitutional state and takes a keen interest in the legal culture. For example, Saarenpää wrote in 2003 how he begins most of his presentations with a discussion of the changes that are taking place in society and the constitutional state. He continued that he has good reason to do so, because the development from the information society to the network society has taken place in a remarkably short time whereas the transition from the traditional - old-fashioned - administrative state to the new modern European constitutional state has been slower¹⁵. In addition, Saarenpää has emphasised that the digital environment is a significant factor in the changes affecting our legal culture. Efforts to achieve an optimal legal culture require a re-evaluation of that culture's components¹⁶. Another focus of research has been the establishment of data systems designed to improve legal operations¹⁷. Changes in the operational environment of legal information and communication have been dealt with by, among other scholars, John Bing¹⁸ and Peter Blume.¹⁹ The above shows that discussion about the changes in society, the constitutional state and the environment in which law operates is still relevant. Some changes still appear only as increased legal information, as good information governance is not firmly rooted enough in the prevailing legal culture.

With reference to reports and relevant court judgments, the paper presents the different phases of asylum procedure in which appropriate information and successful communication have had considerable relevance. These examples show how changes in the operational legal environment within many levels of asylum procedures have not been detected how shortcomings exist in recognising information rights. Hence, fundamental rights are not fulfilled in their entirety.

¹⁴ *Biaudet, Eva* Kansallinen ihmiskaupparaportoiija, kertomus 2010. Ihmiskauppa ja siihen liittyvät ilmiöt sekä ihmiskaupan uhrien oikeuksien toteutuminen Suomessa, 91 -96 (2010).

¹⁵ *Saarenpää Ahti* E-government – Good Government, 303 (2003).

¹⁶ *Saarenpää Ahti* Oikeusinformatiikka. Oikeusjärjestys, osa 1, Lapin yliopisto, 459 (2012).

¹⁷ For example, Magnusson-Sjöberg and Schartum have shown the importance for individuals' rights of issues relating to data systems. *Magnusson-Sjöberg, Cecilia* Rättsautomation: Särskilt om statsförvaltningens datorisering. Stockholm, Norstedts juridik, (1992). *Schartum, Dag Wiese* Rettssikkerhet og systemutvikling i offentlig forvaltning. Oslo, Universitetsforlaget (1993).

¹⁸ *Bing, John* Rettslige kommunikasjonsprosesser: bidrag til en generell teori. Oslo, Universitetsforlaget (1982).

¹⁹ *Blume, Peter* Fra tale til data: studier i det juridiske informationssystem. Akademisk Forlag, København (1989).

2. The heightened salience of information following the expansion of the European Union's competence

The work on the creation of the CEAS started as soon as the Treaty of Amsterdam entered into force in May 1999. Since then, EU and Schengen countries have applied what is known as the Dublin system to identify, register and monitor asylum seekers and illegal immigrants²⁰. This paper focuses on the system only as it affects asylum seekers. According to the European Commission, co-operation of the members states aims to avoid asylum seekers being sent from one country to another and also to prevent abuse of the system. In addition, at least two other background factors have played a role²¹. Dennis De Jong writes that asylum applications tend to be unevenly distributed among member states.²² The situation seemed ideal to test Europe's ability to show solidarity with regard to asylum and immigration policies²³. Secondly, progress in this area accelerated and strengthened due to interests of surveillance: Evelien Brouwer notes that countries in Europe began to emphasise the importance of border monitoring after the terrorist attacks in New York (2001), Spain (2004) and England (2005)²⁴.

The asylum policy of the EU has its legal basis in the primary law and it falls within the area of freedom, justice and security²⁵. The policy is based on solidarity between the member states that ensures fairness towards persons who arrive from outside of Europe. In addition, it is based on the full application of the Geneva Convention relating to the status of Refugees of 28 July 1951, as supplemented by the New York Protocol of 31 January 1967.²⁶ The basis in the Geneva Convention arises also from the CFREU, where the right to asylum is granted in Article 18. The Dublin System consists of the DublinII Regulation, the Eurodac Regulation, and their two implementing regulations²⁷. The related EU directives prescribe the minimum standards for the asylum procedure and reception conditions. In the directives, asylum seekers' rights often appear clearly, precisely and unconditionally.²⁸ The main principle of the Dublin system is that an asylum application is to be lodged in a single member state, that which the applicant first enters. Fingerprints and other personal data of the asylum seeker are collected and entered into Eurodac.²⁹

Eurodac was established by Council Regulation (EC) No. 2725/2000 and it has been operational since January 2003. According to Article 4.1 of the Regulation, member states are required to promptly take fingerprints of every at least 14 years of age in connection with the irregular crossing of an external border of the CEAS. The Commission developed Eurodac and was responsible for the functioning of the Central System as well as the security of the data transfers up to 2012. From 1 December 2012, a new agency for large-scale IT systems has been responsible for the operational

²⁰Regulation (EC) No 343/2003.

²¹For further references, see, e.g., *Staffans Ida*. Evidence in European asylum procedures. Martinus Nijhoff Publishers, Leiden, Boston, 27-33 (2012).

²²In 1997, for example, Germany received 52 per cent of all applications, Greece 1 per cent. See United Nations High Commissioner for Refugees: 1997 Statistical Overview, Statistical Unit (1998).

²³*De Jong, Dennis* Asylum in Europe: Underpinning Parameters. Gordonsville, VA, Palgrave Macmillan, 105 (2003).

²⁴*Brouwer, Evelien* Immigration and Asylum Law and Policy in Europe. No.15 of the Immigration and Asylum Law and Policy in Europe Book Series, Martinus Nijhoff publishers, 30-31 (2008).

²⁵See "Data Processing in European Information Exchange Systems" in *Boehm, Franziska* Information Sharing and Data Protection in the Area of Freedom, Security and Justice –Towards Harmonised Data Protection Principles for Information Exchange at EU-level. Springer Berlin Heidelberg, 259 -318 (2012).

²⁶Article 78 (ex Articles 63, points 1 and 2, and 64(2) TEC) Consolated version of the Treaty on the Functioning of the European Union.

²⁷Commission proposal COM(2008) 825 final 2008/0242 (COD) (Recast version), 4.

²⁸See e.g. Directives 2005/85/EC and 2003/9/EC.

²⁹For further references see, e.g. *Raitio, Juha* A Few Remarks to Evaluate the Dublin System and the Asylum Acquis. T.M.C Asser Press, Springer -Verlag Berlin Heidelberg, the Hague, 111-124 (2011).

management of Eurodac.³⁰ Every year, the authorities of member states record a large number of registry entries in Eurodac³¹. The trend in the number of transactions in the case of asylum seekers increased in 2011 (275,857) compared with 2010 (215,463).³² These numbers do not tell the whole story. Commission has categorised the successful transactions in more detail. Its analysis shows that several persons have more than one hit in Eurodac. One thing that explains these registry entries is that several persons have had to leave the member state which they first entered because of the lack of adequate reception conditions³³.

The Dublin system is built upon the assumption that the asylum procedure and material reception conditions are similar in every member state. In reality, however, there appear to be major differences. Therefore an entry in Eurodac is in fact related to how the rights of asylum seekers are actually realised. For example, if an applicant arrives in Malta, his/her fingerprints and other personal information are stored in Eurodac. If the applicant has to flee inhumane reception conditions in that country and go to some other EU or Schengen country, the earlier entry can still be found. At the worst, an incorrect entry in the register may seriously infringe the rights of an individual. For instance, if the Maltese authorities have registered the age of an applicant incorrectly – a 17-year-old recorded as being 18 – the he or she may be returned to Malta. An under-aged applicant can more easily get a claim to an individual examination in some other country³⁴. Data systems are no longer technical tools for office automation. They have become essential elements of the legal operation of the digital environment.³⁵ If the information rights of individuals are being infringed, at worst some other fundamental rights may be infringed as well.

2.1. Some Examples of the Eurodac database as an Essential Element of Legal Operations

The data stored in Eurodac has had considerable relevance when evaluating the credibility of applicants. For example, The *UK Asylum and Immigration Tribunal* (AIT) gave weight to the Eurodac entry as evidence in *Eritrea v. Secretary of State for the Home Department*³⁶. The AIT noted that the data on the appellant had been recorded in Italy on July 2005, but the appellant denied having left Eritrea before June 2006. The appellant submitted that according to Regulation 2000/2725/ EC, it clearly was contrary to the purpose of the system to use such an item of data to undermine his credibility. Moreover, even if the data was admissible, pursuant to Article 5 of the Regulation there were limits on the types of data which could be stored. In addition, the appellant claimed that the simple printout provided through Eurodac was not sufficient to discharge the burden placed upon the respondent to establish deception or fraud.

³⁰ With a view to achieving synergies, the agency is in responsible also for the operational management of the second generation Schengen Information System (SIS II) and the Visa Information System (VIS). See Regulation (EU) No 1077/2011.

³¹ See e.g. Coordinated Supervision of Eurodac Activity Report 2010-2011 Brussels, (2012). See also *European Data Protection Supervisor* EURODAC Central Unit Inspection Report June 2012, Case file: 2011 -1103 (2012).

³² Annual report to the European Parliament and the Council on the activities of the Eurodac Central Unit in 2011. COM (2012) 533 final, Brussels 5 (2012).

³³ “Why is it that people who had been subjected to the most serious breaches of human rights, and would be in mortal danger if they returned, would prefer ‘to die in Somalia rather than go mad in Hungary.’? For greater detail, see Pro Asyl: Hungary: Refugees between arrest and homelessness, 12- (2012).

³⁴ Compare *Finnish Supreme Administrative Court* cases KHO 14.11. 2010, 2010/2681, and KHO 14.10.2010, 2010/2682, Published in the European Database of Asylum Law <http://m.asylumlawdatabase.eu>.

³⁵ Saarenpää, *Ahti Oikeusinformatiikka*. Oikeusjärjestys, osa 1, 457 (2012).

³⁶ The case was first dealt with in *YI (Previous Claims - Fingerprint match - EURODAC) Eritrea v. Secretary of State for the Home Department*, [2007] UKAIT 00054. AIT ruled that the original Tribunal made a material error of law. See: *RZ (Eurodac - Fingerprint Match - Admissible) Eritrea v. Secretary of State for the Home Department*, [2008] UKAIT 00007, paragraph 56.

The AIT heard testimonies. It was satisfied that the fingerprint evidence from Eurodac was legally admissible - not only when considering which member state is responsible for examining the application for asylum, but also generally as part of the examination of the claim. The AIT stated that this must follow from the clear wording of Article 21(1) of 2003/343/EC, which contains a safeguard that communication of data must be appropriate, relevant and non-excessive for these purposes, but it was not contended that fingerprint evidence either generally or in the particular circumstances of this case contravened these safeguards. The AIT noted that the article also provides that the information held on the system may only be used for the purposes specified and can only be communicated to the authorities, courts and tribunals entrusted with the functions set out in paragraph 7 of the article. The AIT dismissed the appeal on asylum, humanitarian protection and human rights grounds.³⁷

Irish Supreme Court: F. v. Refugee Appeals Tribunal also illustrates the role of Eurodac and shows the importance of information rights. In brief, the appellant said that he had fled Somalia because his tribe was continually being enslaved. He was also kidnapped and imprisoned by the gangs which were part of the militia. For one and a half years, they forced him to work under inhumane conditions. The appellant escaped and first arrived in Malta in 2004. He was imprisoned for about six months and said that he had no opportunity to seek asylum there. The appellant travelled to Finland in February 2005. He applied for asylum, but the application was rejected on the grounds of the DublinII Regulation and he was returned to Malta. From Malta, he was deported to Mogadishu in April-May 2005. The appellant then arranged a trip from Somalia to Ireland. He was caught by authorities when he attempted to enter the UK. An asylum interview was held in February 2006. Again, his asylum claim was rejected. He appealed, and during the court proceedings he told about the itinerary in more detail. According to the appellant it was his first opportunity to tell his story in its entirety. The appellant also said that he feared that he would be sent back to Somalia, whereby in the UK he did not apply for asylum at the first opportunity. The Court rejected the appeal. It stated, among other things, that the contradictions in the account of the journey were not petty in nature³⁸. Violations of the right to information and what effects these had on the case were not adequately addressed, however, as he was not informed about the possibility to lodge an asylum application in Malta in the first instance. Moreover, it seems from the facts of the case that the appellant did not get appropriate information about the system pursuant to valid law either in Finland or Ireland. The ambiguities that appeared were considered without proper investigation merely to reduce the credibility of appellant.³⁹

As the cases show, the Eurodac data system figures as an essential element in the changed operational asylum environment. This emphasises the role of information rights. According to the Data Protection Directive, information processing systems are designed to serve individuals⁴⁰. For example, the European Data Protection Supervisor (EDPS) stated in his opinion in 2011 that the right to information and effective application of this right is significant for the proper functioning of Eurodac. The EDPS continued that it is essential to ensure that the information is given to asylum seekers so that they can fully understand the situation, the extent of their rights and the processes which they may be involved in after administrative decisions. The EDPS pointed out that the right to in-

³⁷ AIT RZ [2008] UKAIT 00007 13-17.

³⁸“Of serious concern to the Commissioner and indeed to the Tribunal are the two Eurodac hits on the applicant, one in Malta and the other in Finland. [...] It was put to the applicant if he had applied for asylum in Malta; he told the Tribunal that he had no chance to do so. [...]” Notice also: “He stated that he had a Solicitor, but I do not believe that he was represented by that Solicitor at the interview.” High Court of Ireland: *F. -v- Refugee Appeals Tribunal* [2008] IEHC 135, 8.5.2008.

³⁹It seems that either the requirements of Geneva Convention were not fulfilled. See in more details about assessment of production of evidence in asylum cases e.g. *Noll, Gregory*, *Evidentiary Assessment Under the Refugee Convention. Risk, Pain and the Intersubjectivity of Fear Procedures*. Nijhoff, Martinus Publishers Leiden, Boston, 141-160 (2005).

⁴⁰Directive 95/46/EC Recital (2).

formation is a cornerstone of data protection legislation and this also is noted in Article 8 of the CFREU⁴¹. Hence, the violations of information rights should also be recognised and infringement should be examined during asylum proceedings. Already the pre-submission guidance in itself is a legal information process. Cases in which applicants do not receive the information they should receive have to be considered as legal questions⁴². Nevertheless, it seems there has been a failure to wake up sufficiently to the importance of information rights and to the importance of enforcing these rights effectively.

3. The Flow of Legal Information – some systematic connections of the Dublin system

The quality standards in information processing also require that authorities be aware of the systemic connections of the database. When the Eurodac database is used, it should also be taken into account that the Dublin system includes, for example, Articles 4 and 19 of the CFREU. The interpretation of both articles leads to an examination of the case-law of the ECtHR regarding Article 3 of the Convention. As stated above, information about the shortcomings of the system has been available aplenty. The Office of the United Nations High Commissioner for Refugees (UNHCR) recommended in 2008 that members refrain from returning asylum seekers to Greece⁴³. In addition, Human Rights Watch published a report in 2008 about the shortcomings in the treatment of unaccompanied migrant children in Greece⁴⁴. Despite the reports, most member states continued to return asylum seekers to what were inhuman and degrading reception conditions.

In this light, *K.R.S v. United Kingdom*, heard before the ECtHR (2.12.2008), can be considered surprising. The applicant in that case complained that he had suffered from inhuman reception conditions in Greece, relying on the reports from high-level agencies and human rights organisations that supported his statement. This notwithstanding, the ECtHR stated that the presumption is that Greece abides by its obligations under Directives 2005/85/EC and 2003/9/EC, which set out minimum standards in asylum procedures and for the reception of asylum seekers.⁴⁵ This position on the protection of fundamental rights is based on the earlier case-law: in *Bosphorus v. Ireland* (30.6.2005)⁴⁶, the ECtHR noted that if a state has engaged with an organisation, and the organisation protects the rights of an individual at least consistently with the ECHR, the presumption is that that state does not infringe its obligations under the Convention if it does no more than implement the judicial obligations related to membership in the organisation. The ECtHR continued that this presumption may be rebutted in a certain case if it appears that the protection is obviously inadequate.

In my opinion, the decision in *K.R.S. v. United Kingdom* is questionable, especially if it is compared to the earlier case-law concerning Article 3; violations have been found in cases where violence was perpetrated by the police⁴⁷, where the space during the custody was too cramped and unsanitary⁴⁸, healthcare was not sufficient⁴⁹ and where the detained person lacked a place to eat and pass the time⁵⁰. Moreover, the Court has stated that an allegation of maltreatment must be examined

⁴¹ Opinion of the European Data Protection Supervisor (2011/C 101/03), 26.

⁴² *Tornberg, Johanna*, Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu, 221 (2012).

⁴³ United Nations High Commissioner of Refugees: UNHCR position on the return of asylum-seekers under the “Dublin Regulation” (2008).

⁴⁴ Human Rights Watch Publications: Left to survive. Systematic failure to Protect Unaccompanied Migrant Children in Greece. (2008).

⁴⁵ Case of *K.R.S. v. The United Kingdom* 32733/08, 2.12.2008.

⁴⁶ Case of *Bosphorus Hava Yollari Turizm Ve Ticaret Anonim Sirketi v. Ireland* 45036/98, 30.6.2005.

⁴⁷ Case of *Emine Yasar v. Turkey* 863/04, 9.2.2010.

⁴⁸ Case of *Skorobogatykh v. Russia* 4871/03, 22.12.2009.

⁴⁹ Case of *Isayev v. Ukraine* 28827/02, 28.5.2009.

⁵⁰ Case of *Tabesh v. Greece* 8256/07, 26.11.2009.

and officials need to show that they do react to alleged infringements. In the earlier case-law, reports of human rights organisations have been taken into account in exercising judicial discretion. In addition, in the *Farbtuhs* case, the ECtHR noted that the ECHR is a living document and it has to be interpreted in the light of present-day conditions. Protection of human rights in terms of the growing requirement level is also important as a possible aggravating factor in terms of Article 3. In other words, certain acts that are otherwise not included in the scope of the article may reach the required harshness. Nonetheless, the authorities have not intervened sufficiently in the case of infringements that asylum seekers have encountered. It should also be taken into account that the ECHR was originally concluded with the specific purpose of protecting everyone's rights, yet for some reason the Court seems to have given co-operation among member states higher priority than the protection of individuals' rights.⁵¹

The Supreme Administrative Court of Finland (SAC) heard a case (2009: 22/440) concerning an applicant's returning to Greece. The applicant had reported that the reception conditions in that country were inhumane. The Finnish Immigration Service stated that it was aware that Greece appeared to have resource problems but that that did not mean the application should be examined in Finland, where better conditions exist for asylum seekers. It noted, as did as the ECtHR, that the presumption of Convention compliance and thus of protection of fundamental rights can be rebutted. Even though the applicant presented claims about infringements, the SAC did not investigate what the reception conditions in Greece were really like. The Court received further clarification only about the asylum procedure in Greece.⁵² However, because the ECtHR had presumed that the directives prescribing the minimum standards have been applied in Greece, it would have been essential for the SAC to explore what possibilities Greece in fact had to offer in the way of accommodation, healthcare and sufficient subsistence. In addition, it should have been taken into account that the relevant directives set out asylum seekers' rights clearly, precisely and unconditionally.

Finally, the ECtHR rejected the return of an applicant to Greece in *M.S.S v. Belgium and Greece* in 2011⁵³. Soon after this decision, the SAC sent a letter to the ECtHR announcing that Finland would examine the cases in which the first fingerprints of applicants had been taken in Greece. However, the presumption of compliance with the directives could already have been rebutted in *K.R.S v. United Kingdom*. Moreover, the SAC could have rebutted the presumption in the 2009 case cited above. The law in force obligates the Court to react immediately as an independent instance if any signs of infringements of an individual's fundamental rights appear. For example, the Swedish Supreme Migrations Court stopped returning asylum seekers to Greece in December 2010, before the decision in *M.S.S. v. Belgium*. That Court examined the reception conditions of Greece through various reports and noted that some European countries were refraining from returns to Greece. It went on to say that in the first instance the national court is the one to rebut the presumption of compliance and, it is not reasonable in the circumstances of asylum seekers that they have to wait for a decision of the ECtHR. Furthermore, the Court ruled, in accordance with the earlier case-law concerning Article 3,⁵⁴ that the prohibition of inhuman treatment should not be applied only in the case of vulnerable groups⁵⁵.

⁵¹ Case of *Polanowski v. Poland*, 16381/05, 27.4.2010, Case of *Khodzhayev v. Russia* 52466/08, 12.5.2010, Case of *Farbtuhs v. Latvia* 4672/02, 2.12.2004.

⁵² KHO 2009: 22/440 1953/1/08.

⁵³ Case of *M.S.S. v. Belgium and Greece* 30696/09, 21.1.2011.

⁵⁴ Compare Case *Gäfgen v. Germany* 22978/05, 1.6.2010“..[T]he prohibition on ill-treatment applied irrespective of the conduct of the victim or the motivation of the authorities; it allowed no exception, not even where the life of an individual was at risk.[..]”.

⁵⁵ For details see MIG 2010:21 UM7706-10. Avdelning 1. Avgörandedatum 10.12.102. Compare MIG 2008:42 UM2397-08.

There has been much legal information available, but information about justice has not always reached the authorities applying the law. Even though the CJEU has clearly ruled that member states are obligated to examine any claim in which an asylum seeker's fundamental rights might be infringed by a Dublin return, the system is still not applied appropriately. In case C-411/10, the CJEU stated that when a regulation confers a discretionary power on a member state, it must exercise that power in accordance with EU law. This underscores that a decision has consequences for that state, which will be bound by the procedural obligations of the EU and by the directives. The CJEU also noted that the member states must not only interpret their national law in a manner consistent with EU law, but also make sure they do not rely on an interpretation of an instrument of secondary legislation which would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles of EU law.⁵⁶ The above examples show that shortcomings appear in the flow of legal information in the new asylum system.

3.1. Some more examples of the need for the further research of dynamic interaction

As Pöysti has written, legal effectiveness requires knowledge about justice; knowledge requires that operators of legal system have systematic legal information as well as theoretical and practical tools to process that information. For the effectiveness of European law, it is essential how legal operators' common body of information is systematised in concrete actions to create a legal system that will be viable in the future.⁵⁷ Examples that are presented in the report of *Still Human Still Here* (SHSH) illustrate systematic shortcomings in the application of legal information, reinforcing Pöysti's observation. In 2010, the SHSH observed that the asylum determination system of United Kingdom gets a quarter of its initial decisions wrong. The success rate at appeal for asylum seekers from certain countries is even higher. In 2008, more than 40 per cent of Eritreans and Somalis appealing against the refusal of asylum won their cases. While many asylum seekers can eventually be granted some form of status, others, particularly those without good legal representation, will get to the end of the process without having their protection needs recognised, and will end up destitute.⁵⁸

Amnesty International has also described how asylum seekers have expressed dissatisfaction at the unfairness and poor quality of the asylum process and, in some cases, the legal advice and representation they have received. The report stresses how rejected asylum seekers are left without reception conditions in the UK, but various infringements of information rights can be recognised as well. For instance, a woman from the Democratic Republic of Congo told how her family were persecuted and subjected to inhuman treatment, with her being raped in front of her six children. She had three legal representatives during the procedure. The first one understood her case, but when she was sent to another part of the country she had to change solicitors. She complained about the interpreting: the interview record showed mistakes and the interpreter's English was poor. In addition, the interviewer and interpreter were men and describing the facts to them was distressing to the woman. Her claim was refused and her second solicitor refused to represent her, demanding a payment. She went alone to her appeal. Her appeal was dismissed and she was destitute, with no friends to help her. She moved from house to house, sleeping on the floor with her son. Other interviewees have reported similar problems. Some found the asylum procedure difficult and were unsure what was expected; some did not even understand the idea underlying the asylum system in the UK.⁵⁹ The Dublin Transnational Network project has also examined asylum processes and notes, among other

⁵⁶Joined Cases C-411/10 and C-493/10, Court of Justice of the European Union, 21.12. 2011.

⁵⁷Pöysti, Tuomas, *Tehokkuus, informaatio ja eurooppalainen oikeusalue*, 5 (1999).

⁵⁸ „This situation has come about partly because of policy decisions to set the bar for protection at the highest level permissible in law, and partly because of problems with a decision-making process that too often denies protection to individuals who are in need of it.” *Still Human Still Here* At the end of the line: Restoring the integrity of the UK's asylum system, 3- (2010).

⁵⁹*Amnesty International* Down and out in London, The road to destitution for rejected asylum, passim (2006).

things, that there are vast divergences in the way the member states apply the system⁶⁰. In summary, the Dublin project has stated how, as a result, a fair and efficient examination of asylum claims is not always guaranteed; having sought protection in Europe, such asylum seekers are often left in a prolonged state of anxiety and uncertainty.⁶¹

The above indicates that asylum procedures' legal effectiveness is not being realised sufficiently. The systematisation of asylum-related information has not enabled concrete actions for the legal systems. Furthermore, the quality of legal representation has varied. In fact, the SHSH considers asylum seekers' early access to good-quality legal advice to be a key element in ensuring that the right decision is made on an asylum application at the first instance. In the UK, the Government has tested the benefits of providing early access to legal advice. Already the first pilot has shown clearly the benefits of the model: applicants got a fairer hearing; cases were decided more speedily; correct decisions were made at an earlier stage; and applicants had more trust in the system.⁶² Unquestionably, good legal advice is significant in safeguarding individuals' rights, including information rights. However, improving legal advice alone cannot replace individuals' information rights: these fundamental rights are not directly proportional to the right of legal advice and have to be realised in any event. The realisation of information rights should not be dependent on who is responsible for disseminating and disclosing the information.

It should also be taken into account that in those member states where the right to a legal adviser is secured already when the responsibility is being determined, applicants usually do not meet their legal advisers during the first registrations⁶³. Even though the legal advisers can later intervene to point out possible errors during registration, errors have sometimes still reduced the credibility of the applicant – regardless of credible reasons for misunderstandings.⁶⁴ It appears that EU's asylum context should also be reviewed with a critical view of the information and communication processes involved. The principles of the constitutional state and judicial inquiry should have guaranteed appropriate application of the legal information, but they have not been enough to secure formal, material and qualitative of legal certainty. There is a need for more concrete tools. A method derived from the theory of information rights and other fundamental rights could offer such a practical tool.

4. Information rights and other fundamental rights in dynamic interaction

Asylum law has frequently been studied in the field of international law or as a part of EU law. As the examples show, the EU's asylum procedures also very much involve an individual's information rights. In the asylum system, where a number of authorities co-operate through the information infrastructure, it is essential that the personal data of an asylum seeker is processed fairly and the right of access to data which has been collected and the right to have it rectified are respected. Applicants also have to receive appropriate information about the operational system and their rights and obligations. Quality asylum procedure presumes successful communication and sound legal information processing by the authorities.⁶⁵ The cases presented above clearly reveal interactions between information rights and other fundamental rights. In this light, methods that draw on legal informatics could be applied alongside those offered by the branches of law cited above.

⁶⁰ See also Gyulai, Gábor/ Roşu, Tudor Structural Differences and Access to Country Information (COI) at European Courts Dealing with Asylum Hungarian Helsinki Committee, Budapest, Hungary (2011).

⁶¹ *Dublin Transnational Project* Dublin II Regulation, Lives on Hold, European Comparative Report, 5 (2013).

⁶² *Still Human Still Here* At the end of the line: Restoring the integrity of the UK's asylum system, 23-24. (2010).

⁶³ *European Union Agency for Fundamental Rights* Fundamental rights at Europe's southern sea borders. Publications Office of the European Union, Luxembourg. (The chapter reviews Greece, Italy, Malta and Spain), 87-89 (2013).

⁶⁴ I base these observations on my previous experience, working as a representative of under-aged asylum seekers and, working by authorization to act as attorney with asylum cases during the years 2009-2013.

⁶⁵ Article 8 (2) Charter of Fundamental Rights of the European Union (2000/C 364/01).

As regards the shortcomings that have been noted, one can see interventions that are essentially related to information rights. For example, the European Asylum Support Office (EASO), which started operating officially in Malta in 2011, undertakes to ensure that individual cases are dealt with a coherent way by different member states. The EASO has described that it applies a bottom-up approach to provide practical support by, among other actions, organising common analysis and common assessment of asylum data and facilitating and stimulating joint action and consistency in the area of asylum procedures. Among other activities, the EASO manages country of origin information (COI) in the EU's common COI portal and promotes training materials in support of the enhancement of quality and harmonisation in the CEAS.⁶⁶ In addition, the Dublin project has adopted measures that reinforce access to understandable information. Part I of the project aimed to strengthen the ability of associations to inform asylum seekers on the process (of being charge of, or taken back) by making information booklets on national asylum systems available. Furthermore, it undertook to provide an individual analysis of asylum seekers' situation in the member state to which they are transferred and, to assure continuity in the legal, social and practical support provided.⁶⁷ Part II of the project has concentrated more on strengthening the structures of the system. First, the project aimed to enlarge the European network in order to improve efficiency and the fairness. Secondly, it sought to deepen the knowledge of those using the asylum system.⁶⁸ The examples dealt with in this paper have shown infringements of information rights that indicate that further research is required. The positive measures reported as well suggest a need for more detailed analyses of the interactions among the fundamental rights⁶⁹.

The foregoing analyses have revealed the broad scope of the phases in the EU asylum procedures in which the information and communication have considerable relevance. Information rights also partly overlap with the other areas of law. This brings challenges for the research task, but these can be addressed in legal informatics. For example, Pöysti has written how the basic legal problem connected to information is that traditional classification used in the field of law and the general doctrines of law cannot effectively identify the basic legal questions related to the use of information and information technology or to the applicable law. Pöysti has classified European information law as a fuzzy set and a dynamic system that interacts with – but does not supplant European - administration law: its functions are partly different, while the reference area often overlaps with it. Information law can be seen as a special system of administration law. However, at the same time it crosses limits and parses information related components comprehensively⁷⁰. The topics discussed in this paper serve to provide a more fine-grained picture of the relevant information law the dynamic involved. Legal informatics offers such a multi-level approach to the rights of asylum seekers. It moves between the general and specific areas of the issue-area and recognises where it overlaps with other branches of law; legal informatics converges with constitutional law and as a field of inquiry becomes superimposed on European administration law. It draws together different strands of research and offers ways to systematise knowledge that address the needs of what is a changed society. The critical approach to information and communication which legal informatics encourages can bring out shortcomings that otherwise are not recognised as efficiently.

The above examples demonstrate that an individual's fundamental rights should not be explored merely as a static factor or by looking at the conflict of rights. The rights should also be viewed in

⁶⁶ Read the tasks of EASO in a nutshell by websites <http://easo.europa.eu/about-us/tasks-of-easo/>.

⁶⁷ Dublin Transnational Project, Part I: <http://www.dublin-project.eu/dublin/Dublin-Project/Dublin-Project-Part-I>.

⁶⁸ Dublin Transnational Project, Part II: <http://www.dublin-project.eu/dublin/Dublin-Project/Dublin-Project-Part-II>.

⁶⁹ See also *European Union Agency for Fundamental Rights* Fundamental rights at Europe's southern sea borders: "Access to reliable information is a precondition for an individual to be able to claim his or her rights. Lack of information makes a person more vulnerable to human rights violations. In the border context, it makes it more difficult for persons in need of international protection to lodge a claim and thus increases the risk of refoulement." Publications Office of the European Union, Luxembourg, 89 (2013).

⁷⁰ Pöysti, *Tuomas* Tehokkuus, informaatio ja eurooppalainen oikeusalue, 536 (1999).

terms of dynamic interaction. My research seeks to create a theory on the dynamic interaction of fundamental rights. The theory differs from the balancing of fundamental rights, where fundamental rights appear “more or less”⁷¹. In a negative dynamic interaction, one right’s success is dependent on the other right’s success. (If right x does not appear, neither does right y.) In a positive dynamic interaction, one right succeeding makes it more likely that another will also succeed. (When right x succeeds, so does right y.) The theory does not claim that any fundamental right is in essence more valuable than any other. There are, however, situations in which the realisation of one right can have a significant impact on the realisation of other rights. The theory will inform a method, or tool, that describes and explains the application and realisation of fundamental rights, or the lack of realisation of these rights. The topic is of heightened importance because particularly important rights can interact in asylum procedures, for example, human dignity, the right to life, integrity, and the prohibition of torture and inhuman or degrading treatment or punishment.⁷²

In the EU asylum procedure, different phases (A), relations (B), effects (C) and variables⁷³ (x^1 x^2) can be distinguished (x^1 -A----- \rightarrow B \leftarrow ----- C - x^2). The method is to first discern the phases in the asylum procedure in which the information rights have had relevance. Second, the norms are identified that safeguard information rights. Third, an analysis is made of the grounds for decisions and whether the decision has possibly affected the realisation of any fundamental rights. Finally, if the case-specific findings show the need for further review, information rights and other fundamental rights are described in terms which make it possible to illustrate interactions between them. Findings that justify this dynamic examination have to be presented as relations, too. The findings can be distinguished in terms of subjective and objective variables. Subjective variables are related to an applicant and indicate, for example, the overall credibility of the application. Objective variables are related to formal elements, for example, the quality of legal advisor and interpreter. The probability of the correctness of the formulating increases, the more accurate information about the variables is available; assumptions can be expressed using less information, but a comprehensive information analysis allows for very cogent arguments. Naturally, in any given case one can discern a number of rights in interaction with information rights and several variables. Effects of interaction may also have different intensities. The focus is not in yielding information that is as exact as possible. Much more important is that the theory would generally increase the knowledge about information rights and that the method would ensure that the awareness of information rights in asylum procedures would be improved. Overall, the aim is to elaborate a method that will provide a corrective of sorts to the application and realisation of fundamental rights, as befits efforts to achieve an optimal legal culture.

5. Conclusions

EU law is based on agreements concluded among member states and it has different starting-points than traditional law of states. EU policy has more visible objectives and legislation is a means to attain these effectively. Scott Shapiro's idea of the law as plans can be seen in such open, target-

⁷¹ The topic has been treated in this publication by Nahabetián Laura Brunet.

⁷² Similar thoughts can already be seen in the Vienna Declaration and Programme of Action 1991, in which was highlighted that CP and ECS rights are equally important and the materialisation of one is linked to that of the other. In addition, especially developing countries have emphasized, how individual human rights can only be realised in a society where individuals, but also different groups, enjoy the economical and social justice and self-determination. *Ministry of Foreign Affairs of Finland Democracy and Human Rights - A pathway to peace and development*. 4 (2000).

⁷³ In a number of researches the legal phenomenon has been distinguished to the separate questions. See e.g. *Zitting, Simo Omistajanvaihdoksesta silmällä pitäen erityisesti lainhuudatuksen vaikutuksia*. Suomalainen lakimiesyhdistys, Helsinki, 109- (1951).

oriented co-operation⁷⁴. Yet, EU law is also built on the common constitutional traditions of the member states. The law of any state is more than just a collection of plans. In addition to creating and maintaining a welfare state, national law provides for order and the protection of individuals from unlawful interference by the authorities. EU law aims for building legal framework with the member states' legal systems. In asylum issues this is seen in a very significant way: the plan for the return of an asylum seeker may not be enforced if this would infringe an applicant's fundamental rights. EU law in the abstract has not interacted appropriately with the concrete application processes of asylum; interpretations are not always sought systematically from the abstract legal order⁷⁵. Here one sees clear evidence of the slow pace of change towards the European constitutional state.

If one looks at EU legislation, it is clear that the changes in the system were not intended to break the coherence of the system. The Dublin system is based on legal rules and principles which prescribe that every decision has to take into account individuals' fundamental rights. However, in the case of asylum in the EU, it seems that the situation has developed in a direction which in other, similar contexts has prompted concern for scholars in legal informatics: National authorities have often applied the Eurodac database alone; the Dublin system, as a larger legal framework, has not been considered sufficiently. The DublinII Regulation has often been detached from its legal context and its basis in the primary law and the specific interpretation the rules of EU law have not been taken into account. The directives, which seek to protect asylum seekers rights, have contrary to this purpose, been used as a formal justification for decisions, although the rights set out in the instruments are not in practice observed in all member states. Even though the principle of judicial investigation is binding in EU asylum cases, authorities have not been aware of the rules of interpretation in what is a changed system.

There is every argument for preventing abuses of the asylum system efficiently. Justifiable transfers of applicants to another member state should be distinguished from insincere transfers. Infringements are serious and therefore it is not sufficient to intervene in these cases only in the future. Those applicants who are in danger of being returned or have already been returned to what are inhumane reception conditions should get protection retroactively. All legal subjects of the primary law should be equally protected when rights are created and enshrined in the Treaties or instruments derived from the Treaties. Several rights of asylum seekers appear clearly, precisely and unconditionally in the secondary legislation⁷⁶. It should also be taken into account that discrimination on the basis of nationality is prohibited within the scope of application of the Treaties. It is not sufficient that discrimination is prohibited among EU citizens only. However, human dignity and the other guaranteed rights and freedoms are not granted in a similar way to people who come from outside of Europe - despite the fact that these rights are derived from hierarchically equal sources of law. These requirements are justified, because member states have been given powers in keeping with the principle of subsidiarity with a view to establishing a common legal asylum system. If the doctrine of EU law is different in the purview of Treaties only because of nationality, the status of the legal subjects is unequal in the scope of primary law. In that case, the basis for the common asylum policy in the Treaties and the position of unilateral acts derived therefrom as a part of binding EU law is very questionable. It is also to be taken into account that the principle of solidarity is binding. Moreover, the Commission has urged the member states to show solidarity towards those states whose asylum systems are under pressure. The Dublin system has to be discussed in light of the

⁷⁴ I view Shapiro's theory as an approach of the actor of the legal system to the question of „what is law?“ *Shapiro, Scott* Legality. Harvard University Press (2011).

⁷⁵ Tolonen views the sources of law through the concept of objectivation. He describes law as a social and cultural interaction process between structures and actors. In this interaction, law has two forms: concrete and abstract. I understand the perspective of Tolonen as an internal approach of the legal system to the question of „what is law?“. *Tolonen, Hannu* Oikeuden kaleidoskooppi kirjoituksia oikeudesta ja sen historiasta. Suomalainen lakimiesyhdistys, Helsinki 156- (2008).

⁷⁶ See for direct effect case *Van Gend en Loos v Nederlandse Administratie der Belastingen*, Case 26/62, 1963.

concept of good information governance, which is set out in legislation, with appropriate reference to discussions of case-law.

Clearly, the Eurodac database is more than a technical tool, as registry entries have been given significant value during essential legal operations. In the digital environment, enforcing the right to functional data bases is fundamental. According EU law, the authorities' role is that of an active, enforcing, advisory and informative party in the procedure. Officials have to collect and store information appropriately, tell why such sensitive data is collected, where it is used and what impacts this has; in addition, the data transfers have to be secured. The use of the database needs to be situated in the larger legal framework. This concerns a requirement that authorities be aware of the all systematic connections of the data base. However, the flow of legal information has often failed in the asylum cases of EU – despite the fact that the CEAS acquis demonstrates plainly the legal basis on which the system was intended to apply. Moreover, the instruments of international law clearly state that the rights of individuals are to be protected; for example, the prohibition against inhuman treatment contained in Article 3 of the ECHR is absolute. The reports do not leave a reasonable doubt about the inhumanity of reception conditions, but the court decisions have not been fair to the legal subjects concerned. Luckily a number of high-level agencies and human rights organisations have woken up to the infringements that have occurred in the changed system. Nonetheless, awareness otherwise has increased very slowly. The mechanism allowing temporary suspension of transfers was added late and it has not been effective⁷⁷. Also discussions concerning enhanced intra-EU solidarity have progressed slowly⁷⁸. In addition, the EASO, mentioned above, did not become operational as an EU agency until 2011.

A critical approach to information and communication covering the entire asylum procedure also brings out the questions concerning the validity of the information that human rights organisations and high-level agencies produce, the use and scope of country information⁷⁹ and, deficiencies in communication with the parties. Furthermore, the findings also show that the violations of information rights are not identified sufficiently. Therefore, information rights need to be highlighted as fundamental rights and infringements should be examined with due effectiveness. This approach also makes it possible to explore different models of legal planning that arise from legislation and to search for models introduced in the literature. The appropriate early design of the data system would have enabled comprehensive risk assessment and, risk management mechanisms should be included in the system by design⁸⁰. According to the sources, the impossibility of the CEAS could not come as a surprise. As De Jong has noted, the travel routes of Kurds asylum seekers were clearly demonstrated to pass through Greece, but in the political debates centralisation of the reception was never seriously considered. De Jong remarks that by dealing with the issue openly and admitting that responsibility passed mainly to Greece and Italy would have achieved much more; to initiate the real burden-sharing discussions, for example, the technical and economic support could have been organised by the EU mechanisms, but also on a bilateral basis bilaterally⁸¹. The model whereby the mere political authority has been sufficient to create a binding legal order, which has essentially impacts on the fundamental rights of individuals, requires closer inspection. It was clear when the system was created that it could not be adequately applied everywhere as a legal system due to lack of resources. Therefore, there one has to pose the question whether the protection of individuals' rights requires legally binding guarantees requiring that comprehensive assessments of the real functioning of the system be carried out before establishing new systems. Although the legal order

⁷⁷ See Opinion of the Committee of the Regions (2012/C 277/03).

⁷⁸ Proposal COM(2008) 820 final.

⁷⁹ See e.g. *Gyulai, Gábor* Country Information in Asylum Procedures -Quality as a Legal Requirement in the EU. Updated version, 2011 Hungarian Helsinki Committee, Budapest, Hungary (2011).

⁸⁰ Proposal COM/2012/011 final - 2012/0011 (COD), Article 23 "Data protection by design and by default".

⁸¹ *De Jong, Dennis* Asylum in Europe: Underpinning Parameters. Gordonsville, VA, USA Palgrave Macmillan, 110 (2003).

clearly prescribes coherence with the earlier system – this cannot in itself guarantee that the new system will be applied as a robust legal system.

Already the pre-submission guidance in itself is a legal information process. Cases in which applicants do not receive the information they should receive have to be considered as legal questions. A communicative approach to the nature of law clarifies the significance of information; law appears as information⁸². It seems that there has been much quality legal information available, but not enough legal knowledge about the changed system, or perhaps little will to apply the system equitable in asylum cases. This has led to serious infringements of individuals' rights as well as systematic deficiencies in asylum procedures, causing legal inefficiency. Matters that should have been familiar already on the basis of the old operational environment are still not perceived enough. Moreover, there has been a failure to notice that the special cooperation between the member states authorities has largely changed the operational environment of asylum cases. Authorities' evaluation and argumentation has sometimes wrongly proceeded in terms of the old environment. The changes that the digital environment has caused in the asylum context are considered often only as changes in norms but good information government has not been assimilated into the legal culture.

There has been a failure to observe the new context of EU asylum law as a whole. Operating in too narrow legal environment with inadequate legal knowledge has led to serious infringements being approved "legally", despite the safeguards for individuals prescribed in EU law, but also national constitutions and international instruments have been ignored. Merely by interpretations of the laws that further fundamental and human rights, one would have concluded that nobody should be returned to a country where inhuman reception conditions appear. Especially when a system undergoes changes, administration of justice and the effects thereof should be reviewed critically. Regardless of the level at which the legislation has been adopted – national, EU or international – officials cannot avoid their responsibility as those who apply the law. For some reason, it has not been clear that the changed asylum system is also a legal system. There is a need for more concrete tools. A method derived from the theory of information rights and other fundamental rights could offer such a practical tool.

6. References

Aarnio Aulis Tulkinnan taito: ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. WSOY, Helsinki (2006).

Amnesty International Down and out in London, The road to destitution for rejected asylum seekers. http://www.amnesty.org.uk/uploads/documents/doc_17382.pdf last accessed 10.4.2013 (2006).

Amnesty International Seeking safety, finding fear: Refugees, asylum-seekers and migrants in Libya and Malta. <http://www.amnesty.org/en/library/asset/REG01/004/2010/en/d0e71b60-71ec-4c4b-8b2f-d03a881b90f6/reg010042010en.pdf> last accessed 12.6.2013 (2010)

Amnesty International: The Dublin II trap, transfers of asylum-seekers to Greece <http://www.amnesty.org/en/library/asset/EUR25/001/2010/en/e64fa2b5-684f-4f38-a1bf-8fe1b54d83b5/eur250012010en.pdf> last accessed 10.4.2013 (2010).

Biaudet, Eeva Kansallinen ihmiskaupparaportoiija, kertomus 2010. Ihmiskauppa ja siihen liittyvät ilmiöt sekä ihmiskaupan uhrien oikeuksien toteutuminen Suomessa (2010).

Bing, John Rettslige kommunikasjonsprosesser: bidrag til en generell teori. Universitetsforlaget, Oslo (1982).

⁸² I view the question of „what is law ?“ from different approaches. These approaches can also be described in different abstraction levels. In addition to above mentioned, I also understand that law has a core area, which concerns the question of morality.

Blume, Peter Fra tale til data: studier i det juridiske informationssystem. Akademisk Forlag, København (1989).

Boehm, Franziska Information Sharing and Data Protection in the Area of Freedom, Security and Justice –Towards Harmonised Data Protection Principles for Information Exchange at EU-level. Springer Berlin Heidelberg (2012).

Brouwer, Evelien Immigration and Asylum law and Policy in Europe. In: Nijhoff, Martinus (ed.) Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System. No.15 of the Immigration and Asylum Law and Policy in Europe Book Series, Martinus Nijhoff publishers (2008).

Coordinated Supervision of Eurodac Activity Report 2010-2011 Brussels, 24 May 2012 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/12-07-04_EURODAC_Activity_Report_EN.pdf last accessed 25.5.2013 (2012).

De Jong, Dennis Asylum in Europe: Underpinning Parameters. In: Joly, Daniele (ed.) Global Changes in Asylum Regimes. Gordonsville, VA, USA: Palgrave Macmillan (2003).

Dublin Transnational Project Dublin II Regulation: Lives on Hold, European Comparative Report. February 2013 <http://www.ecre.org/component/content/article/56-ecre-actions/317-dublin-ii-regulation-lives-on-hold.html> last accessed 4.6.2013 (2013).

European Commission Report from the Commission to the European Parliament and the Council Annual report to the European Parliament and the Council on the activities of the EURODAC Central Unit in 2011 <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0533:FIN:EN:PDF> last accessed 4.6.2013 (2011).

European Data Protection Supervisor EURODAC Central Unit Inspection Report June 2012 Case file:2011-1103 http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/12-06-14_EURODAC_inspection_report_EN.pdf last accessed 24.5.2013 (2012).

Eurodac Supervision Coordination Group: Recommendations on the use of DubliNet https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Eurodac/10-06-28_DubliNet_recommendations_EN.pdf last accessed 28.5.2013 (2010).

European Union Agency for Fundamental Rights Fundamental rights at Europe's southern sea borders. Publications Office of the European Union, Luxembourg. http://fra.europa.eu/sites/default/files/fundamental-rights-europes-southern-sea-borders_en.pdf last accessed 30.6.2013 (2013).

Gyulai, Gábor Country Information in Asylum Procedures -Quality as a Legal Requirement in the EU, Updated version. Hungarian Helsinki Committee, Budapest, Hungary http://helsinki.hu/wp-content/uploads/EN_COI-in-Asylum.pdf last accessed 3.6.2013 (2011).

Gyulai, Gábor/ Roşu, Tudor Structural Differences and Access to Country Information (COI) at European Courts Dealing with Asylum. Hungarian Helsinki Committee, Budapest, Hungary. http://helsinki.hu/wp-content/uploads/EN_Structural-differences-and-access-to-country-information-COI-at-European-courts-dealing-with-asylum.pdf last accessed 3.6.2013 (2011).

Irish Refugee Council/ NGO Forum on Direct Provision Direct Provision and Dispersal: Is there an alternative? <http://irc.fusio.net/wp-content/uploads/2011/09/Direct-Provision-and-Dispersal-Is-there-an-alternative.pdf> last accessed 15.5.2013 (2011).

Maahanmuuttovirasto (Finnish Immigration Service), Turvapaikkayksikön tilastokatsaus http://www.migri.fi/download/39964_tupa_tilastokatsaus_2012.pdf last accessed 20.3.2013 (2012).

Maahanmuuttovirasto (Finnish Immigration Service) Turvapaikkayksikön tilastokatsaus

http://www.migri.fi/download/31527_tilastokatsaus_2011_tupa_valmis.pdf last accessed 20.3.2013 (2011)

Magnusson-Sjöberg, Cecilia Rättsautomation: Särskilt om statsförvaltningens datorisering. Norstedts juridik, Stockholm (1992).

Ministry of Foreign Affairs of Finland Democracy and Human Rights - A pathway to peace and development (2000).

Noll, Gregor (auth./ed.): Evidentiary Assessment Under the Refugee Convention. Risk, Pain and the Intersubjectivity of Fear. In: Proof, Evidentiary Assessment and Credibility in Asylum Procedures. Martinus Nijhoff Publishers Leiden, Boston 141-160 (2005).

Pro Asyl: Hungary: Refugees between arrest and homelessness, Report on year-long research up to February 2012 http://bordermonitoring.eu/files/2012/11/BM_Hungary_English.pdf last accessed 29.3.2013 (2012).

Pro Asyl The Living Conditions of Refugees in Italy. A Report by Maria Bethke & Dominik Bender. Report on the research trip to Rome and Turin in October 2010. Frankfurt am Main, 28.2.2011. Translation of the German original text published on 28.2.2011; Susanna Thomas. http://www.proasyl.de/fileadmin/fm-dam/q_PUBLIKATIONEN/2011/Italyreport_en_web_ENDVERSION.pdf last accessed 29.3.2013 (2011).

Pöysti Tuomas, Tehokkuus, informaatio ja eurooppalainen oikeusalue. Helsingin yliopisto, Yliopistopaino (1999).

Raitio, Juha A Few Remarks to Evaluate the Dublin System and the Asylum Acquis 111-124 in: Goudappel, Flora A. N. J./ Raulus, Helena S. (eds.) The Future of Asylum in the European Union: Problems, Proposals and Human Rights. T.M.C Asser Press, Springer -Verlag Berlin Heidelberg, the Hague (2011).

Saarenpää, Ahti Kadonneet systeemit. In: Minun Metodini. Häyhä, Juha. (ed.) Werner Söderström lakitieto, Helsinki (1997).

Saarenpää, Ahti Oikeusinformatiikka. In: Oikeusjärjestys, osa 1, Tammilehto, Timo (ed.) Lapin yliopisto (2012).

Schartum, Dag Wiese Rettssikkerhet og systemutvikling i offentlig forvaltning. Universitetsforlaget, Oslo (1993).

Shapiro, Scott Legality. Harvard University Press (2011).

Staffans Ida Evidence in European asylum procedures. Martinus Nijhoff Publishers, Leiden, Boston (2012).

Still Human Still Here At the end of the line: Restoring the integrity of the UK's asylum system <http://stillhumanstillhere.files.wordpress.com/2009/01/at-the-end-of-the-line-2010.pdf> last accessed 19.4.2013 (2010).

Tolonen, Hannu Oikeuden kaleidoskooppi kirjoituksia oikeudesta ja sen historiasta. Suomalainen lakimiesyhdistys, Helsinki (2008).

Tornberg, Johanna Edunvalvonta, itsemääräämisoikeus ja oikeudellinen laatu. Lapin yliopisto-kustannus, Rovaniemi (2012).

United Nations High Commissioner for Refugees 1997 Statistical Overview Statistical Unit, (1998)

United Nations High Commissioner for Refugees Regional Representation for Central Europe, Refugee Homelessness in Hungary. Budapest, Hungary, March 2010 <http://www.refworld.org/cgi-bin/txis/vtx/rwmain?docid=4bb4b9ac2> last accessed 17.5 2013 (2010).

United Nations High Commissioner of Refugees UNHCR position on the return of asylum-seekers under the “Dublin Regulation” 15 April 2008 <http://www.unhcr.org/refworld/docid/4805bde42.html> last accessed 22.4.2013 (2008).

Zitting, Simo Omistajanvaihdoksesta silmällä pitäen erityisesti lainhuudatuksen vaikutuksia. Suomalainen lakimiesyhdistys, Helsinki (1951).

CATEGORIZING BIOMETRIC APPLICATIONS

Juhani Korja

Researcher, Labour Law and Social Law,
University of Lapland, Finland
juhani.korja@ulpland.fi

Keywords: *Biometrics*

Abstract: *Identification is a fundamental component of human interaction. The traditional means of identification, i.e. ID cards and passports, have been the most widely used, and are likely to remain as such for years to come. However, stronger identification technologies, such as biometrics, are becoming commonplace. According to the American Heritage Dictionary, the term biometrics has traditionally stood for “the statistical study of biological phenomena.” Because of the growing usage of automated systems for person identification by government and industry, the term “biometrics” now commonly refers to “automated methods for recognition or verification to determine the identity of a person based on physiological or behavioral characteristics.” In this article I will examine the ways biometric applications can be categorized. I will examine how the biometrics can be categorized. I will also examine some of the societal issues which are related to the deployments of biometric identification.*

1. Introduction

Identification is a fundamental component of human interaction. The traditional means of identification, i.e. ID cards and passports, have been the most widely used, and are likely to remain as such for years to come. However, stronger identification technologies are becoming commonplace. Biometric identification is one such technology.

According to the American Heritage Dictionary, the term biometrics has traditionally stood for “the statistical study of biological phenomena.”¹ Because of the growing usage of automated systems for person identification by government and industry, biometrics is now commonly refers to “automated methods for recognition or verification to determine the identity of a person based on physiological or behavioral characteristics.”²

The reason for the vast growth of biometric technologies is simple. Biometrics have been made possible by explosive advances in computing power. It should also be noted that biometrics is seen as the silver bullet for terrorism. The utilisation of biometric technology enables automation in identification and thus makes identification more accurate and effective.

¹ The American Heritage Dictionary. Available at: <http://www.ahdictionary.com/word/search.html?q=biometrics>.

² Sethi, I: Biometrics. Overview and Applications, p. 117.

Since the late 1990s - four factors, reduced cost, reduced size, increased accuracy and increased ease of use – have combined to make biometrics an increasingly feasible solution.³ The terrorist act of September 11th has been another major factor spurring innovation in biometric applications. But it should be mentioned that biometrics are much more than a replacement for the traditional identification methods. Millions of people use biometric technology in applications as varied as time and attendance, voter registration, international travel and benefits dispersal. Biometrics can be used for security, for fraud reduction, for convenience, even as an empowering technology, depending on the application.⁴

2. What is biometric identification?

Biometric identification is the automated use of physiological or behavioural characteristics to determine or verify identity.⁵ The automated use means that in the identification process computers or machines are used to verify or determine identity through behavioural or physiological characteristics. Because the process is automated, biometric identification generally requires only a few seconds, and biometric systems are able to compare thousands of records per second.

With a range of available attribute choices, a question arises: What are the desirable characteristics of a biometric attribute for automatic identification? The answer is distinctiveness, robustness and measurability. These characteristics are deemed most important. Distinctiveness implies that the attribute must show great variability over the general population so as to yield a unique signature for each individual. Robustness determines how the attribute varies over time. Ideally it should not change over time. The measurability refers to the ease with which it can be sensed.⁶

³ According to Ishwar Sethi, a number of factors have led to the unprecedented growth of biometrics. Chief among them are decreasing hardware costs, growth in networking and e-commerce, and greater emphasis on security and access control. Sethi, I: Biometrics. Overview and applications (2006), p. 118.

⁴ India has deployed the world's largest biometric identification program. The idea of the program is to register every citizen's fingerprint into a registry, and replace passports and other ID cards as an identification method. BBC News, available at <http://www.bbc.co.uk/news/world-asia-india-16979875>.

⁵ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002). According to The Council of the EU's Glossary of Security Documents, Security Features and other related technical terms, biometrics is defined accordingly: A personal biological (anatomical or physiological) or behavioural characteristic which can be used to establish a person's identity by comparing it with stored reference data. The Council of the EU. Glossary of Security Documents, Security Features and other related technical terms, available in English at: <http://prado.consilium.europa.eu/en/glossarypopup.html>

It can be said that the most popular biometric identifier is the fingerprint. Other frequently used biometric identifiers are facial image, iris image and hand geometry. Biometric identifiers can be used for biometric recognition processes such as *facial* and *iris recognition*. The term "biometrics" is used to denote the method of measuring biometric identifiers.

⁶ Wayman, J.L.: Fundamentals of Biometric Technologies, available at http://www.engr.sjsu.edu/biometrics/publications_tech.html. See also Sethi, I: Biometrics: Overview and Applications (2006).

In addition, it is desirable that the attribute is acceptable and universal. The acceptability implies that no negative connotation is associated with it. The universality of an attribute determines the fraction of the general population that possesses it in multiples.⁷

Based on the features used, the biometric technologies can be divided into two different categories:

- 1) Physiological biometric identification, wherein the identification is based on a physiological feature, such as a fingerprint or a facial image.
- 2) Behavioural biometric identification, wherein the identification is based on a behavioural feature.⁸ Behavioural characteristics are action or dynamic attributes and have an element of time associated with them. Examples of such attributes used by biometric systems include signature, voice, and keystroke pattern.

3. Defining the biometric applications

Just as leading biometric technologies differ in fundamental ways, the major biometric applications differ substantially in terms of security and convenience requirements, process flow of enrolment and verification and system design. In order to deploy biometrics effectively, one must understand the dynamics of the specific application deployed.

Traditionally, biometric applications are divided into three categories:

- 1) Applications in which biometrics provide **logical access** to data or information
- 2) Applications in which biometrics provide **physical access** to tangible materials or to controlled areas
- 3) Applications in which biometrics **identify or verify the identity** of an individual from a database or token⁹

These categories indicate the most basic differences among those in which biometrics can be deployed. However, they fail to capture a number of application-specific factors that are critical to understanding biometrics:

- In what manner does the individual interact with biometric system?
- Does the user claim identity before interacting with the system?
- Is the user motivated to comply with the biometric system?
- What is the value of the data or materials the biometric is protecting?

After considering how biometric applications differ according to these criteria, two types of categorization take shape, which both have seven classifications. First there is the application-based categorization.

- 1) Criminal identification

⁷ Wayman, J.L.: Fundamentals of Biometric Technologies, available at http://www.engr.sjsu.edu/biometrics/publications_tech.html. See also Sethi, I: Biometrics: Overview and Applications (2006). *ibid*.

⁸ See more about biometric technologies i.e. Bolle, R – Connell, J – Pankanti, S – Ratha, N – Senior, A: Guide to Biometrics (2004) and Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity Verification in a Networked World (2002).

⁹ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity Verification in a Networked World (2002).

Criminal identification is the use of biometrics to identify or verify the identity of a suspect, detainee or individual in a law enforcement application.¹⁰ The primary role of the biometric is to identify an individual in order to proceed with or halt a law enforcement process. It should be noted that without biometrics it might be impossible to reliably identify a suspect.

Criminal identification was the first widespread use of biometric technology. Over 35 years, automated fingerprint searches against local, state, and national databases, as well as automated processing of mug shots, have become pervasive criminal identification applications, used around the world.

2) Retail/ATM/point of sale

Retail/ATM/point of sale is the use of biometrics to identify or verify the identity of individuals conducting in-person transactions for goods or services. The biometric is used to complement or replace identification methods such as pins and identification cards.¹¹

3) E-commerce

E-commerce is the use of biometrics to identify or verify the identity of individuals conducting remote transactions for goods or services. The biometric is used to complement or replace mechanisms such as passwords and PINs.¹²

To this point there has been no typical e-commerce application, as there are few commercial Web sites that utilize biometric identification for customers or clients

4) PC/network access

PC/network access is the use of biometrics to identify or verify the identity of individuals accessing PCs, PDAs or networks. The biometric is used to replace passwords and tokens.¹³ This application is closest to traditional logical access because its purpose is to grant access to a resource.

Currently there are many applications that are fully addressed by PC/network access. For instance, some laptop computers (i.e. Dell) have finger-scan as an option for logging on to the laptop.

5) Physical access/time and attendance

Physical access/time and attendance is the use of biometrics to identify or verify the identity of individuals entering or leaving an area at a given time. Time and attendance is frequently deployed in conjunction with physical access. While these are two separate applications, physical access and time and attendance are linked. The reason they are linked is simple: both pertain to restricting or controlling the presence of an individual within a given space.¹⁴

Currently there are many applications using biometric technology. For example in Hyvinkää, a municipal town in Finland, a gym has deployed a fingerprint based biometric system for

¹⁰ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002). p. 144.

¹¹ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002), p. 144.

¹² Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002), p. 145.

¹³ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002), p. 145.

¹⁴ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002), p. 145.

checking in and in the Bergen airport it is possible to board a plane using finger-scan. Also worth mentioning is that the US Department of Homeland Security is using fingerprint technology applications to register and verify visitors from abroad.

6) Citizen identification

Citizen identification is the use of biometrics to identify or verify the identity of individuals in their interactions with government agencies for the purposes of card issuance, voting immigration, social services, or employment background checks.¹⁵

A wide range of interactions between individuals and governments is captured under the citizen identification. Biometric technology is used to facilitate border crossing for citizens, for passport issuance and processing and to verify the identity of refugees.¹⁶

7) Surveillance¹⁷

Surveillance is the use of biometrics to identify or verify the identity of individuals present in a given space. Surveillance differs from physical access/time and attendance inasmuch as surveillance does not assume user compliance.¹⁸ Surveillance also has dramatically different requirements in terms of accuracy and enrolment and verification processes.

Biometric surveillance systems are deployed in the majority of the major casinos in North America and in a handful of police applications to search passers-by or event attendees against hit lists of known criminals¹⁹. Depending on the results of the first few surveillance implementations, surveillance may become a widely deployed technology.

Another way of categorizing biometric applications has been presented by Dr. Jim Wayman, Director of the National Biometric Test Center at San Jose State University. He lists seven different modes of applying or characterizing a biometric application.²⁰ These modes are

¹⁵ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002). p. 157

¹⁶ Iris recognition technology is being used for passenger authentication programs at selected airports in the US, UK, Amsterdam, and Iceland. At border crossings in Canada, the Netherlands, and the United Arab Emirates, iris recognition is being used to help registered travelers cross borders without passing through lengthy immigration checks and lines. Iris recognition technology is also being used in Pakistan to identify and track Afghan refugees in the camps run by the Office of the United Nations High Commissioner for Refugees (UNHCR)

¹⁷ The list presented here is not final. It is just one way of categorizing biometric applications. The list was first presented by Nanavati, S – Thieme, M – Nanavati, R in their publication Biometrics. Identity Verification in a Networked World (2002). Another way to categorize biometric applications has been presented by Ishwar Sethi. According to Sethi biometric applications can be grouped into 1) access control and attendance (controlling access to physical locations, replacing time punch cards), 2) computer and network access control, 3) Financial and health services (ATM's), 4) Government (immigration, border control), 5) Law enforcement (surveillance, criminal identification) and 6) telecommunications. Sethi, I: Biometrics: Overview and Applications (2006), p. 129. Both of these ways have taken into account the possible ways, how biometrics can be deployed. However, Nanavati et al, have more profound way to categorize biometric technologies. This is because they also take into account the various vertical markets (Law enforcement, government sector, financial sector, healthcare and travel and immigration) in which biometrics are deployed effectively, and these markets share a common need for biometrics in areas such as health care and financial services.

¹⁸ Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a networked world (2002)

¹⁹ For example, immigration officials in Massachusetts are using face recognition to prevent duplicate green card applications. In Pinellas County in Florida, face identification is being used to identify criminals.

²⁰ Wayman, J.L.: Fundamentals of Biometric Technologies, available at: http://www.engr.sjsu.edu/biometrics/publications_tech.html.

categorized according to the biometric system design, and describe how the biometric systems can be deployed.

These are:

1) Overt or covert

This mode of application refers to whether the biometric data is being captured with the consent and awareness of the subject. The most common mode is the overt mode. Some biometric systems, however, can be operated in covert mode. For example, face recognition offers a convenient way of operating in covert mode because a person's face can easily be captured without the subject's awareness.

2) Cooperative or non-cooperative

The distinction between cooperative and non-cooperative deployment refers to how an imposter will try to defeat the system. Will the imposter gain access by cooperating with the system to get a positive match, or will the imposter try to avoid a match by not cooperating with the system?

3) Habituated or non-habituated

A habituated deployment of a biometric system implies that the users come in contact with the system frequently while non-habituated deployment means that users only occasionally access the system.

4) Supervised or unsupervised

The supervised/unsupervised distinction concerns whether an operator is present to ensure the proper capturing of biometric data. This distinction can also be referred to as attended/unattended.

5) Closed or open

This deployment refers to how the biometric templates are going to be used. A closed deployment means that the template database is used only for a single application for which it was created. An open deployment means that the template database is available for multiple applications.

6) Public or private

The public or non-public distinction refers to the relationship between the users and the management of the biometric system. If the system is operated for employees of an organization, it is a private deployment. Whereas, in a public deployment the users are the clients or customers of the organization.

7) Standard or non-standard environment.

The standard versus non-standard distinction tells us about the deployment environment. When the system is deployed in a controlled environment, it is considered a standard application; otherwise it is a non-standard application.

In addition to the aforementioned categories, a large percentage of biometric deployments are also used within five sectors or markets. These could be called biometric verticals. These sectors

or markets may be characterized by an inherent need for user identification or by the presence of valuable or sensitive data. In these verticals, biometrics can serve to increase security or reduce fraud, and they may provide functionality not achievable through other authentication methods.²¹

It should be noted that while almost every biometric deployment can be categorized according to technology and application, vertical analysis cannot account for all biometric sales. A fair percentage of biometric usage cannot be classified according to a particular market. Because of this, discussion of five key verticals is a more reasonable approach.²²

Law enforcement: The law enforcement sector includes the use of biometrics to identify the identity of individuals apprehended or incarcerated because of criminal activity, suspected of criminal activity, or whose movement is restricted as a result of criminal activity. Typical law enforcement deployments include AFIS²³, surveillance, mug shot processing through facial-scanning, corrections (finger-scan and iris-scan), and probation/home incarceration applications.

Government sector: The government-sector includes the use of biometrics to identify the identity of individuals interacting with a government entity or acting in the capacity of a government employee official. Typical government-sector deployments include national IDs, driver's licenses, benefits distribution, employee authentication, and military usage.

Financial sector: The financial-sector includes the use of biometrics to identify the identity of individuals interacting with a financial-sector entity or acting in the capacity of a financial-sector employee. Banking and financial services represent enormous growth areas for biometric technologies. Financial sector deployments incorporate both customers and employees, and range from internal deployment to remote and kiosk-based authentication. As of early 2001, finger-scan, facial-scan, and retina-scan have been deployed successfully by financial institutions worldwide for transaction authentication, access to computers and networks, and physical access.

Healthcare: The healthcare sector includes the use of biometrics to identify the identity of individuals interacting with a healthcare entity or acting in the capacity of a healthcare employee or professional. Typical healthcare deployments include PC/network access, access to personal information, and patient identification.

Travel and immigration: This sector includes the use of biometrics to identify the identity of individuals interacting, during the course of travel, with a travel or immigration entity or acting in the capacity of a travel or immigration employee. Travel and immigration deployments can incorporate citizens, employees, or customers in the form of travellers, with leading applications including air travel, border crossings, employee access, and passports.

The three roles in which an individual encounters biometrics

The role a person occupies when interacting with a biometric system is an often overlooked but essential determinant of such factors as privacy, accuracy and performance²⁴. An example is in

²¹ Nanavati, S. – Thieme, M. – Nanavati, R.: Biometrics Identity Verification in a Networked World (2002), p. 209-233. Also gaming and education verticals are well suited to biometric authentication. In gaming applications biometrics have found a steady foothold in many major casinos. In education, the need to authenticate students and guardians has led to some interesting deployments of biometric technology. See more: Nanavati, S. – Thieme, M. – Nanavati, R.: Biometrics. Identity Verification in a Networked World (2002), p. 232-233.

²² Nanavati, S. – Thieme, M. – Nanavati, R.: Biometrics. Identity Verification in a Networked World (2002), p. 210.

²³ AFIS is an abbreviation from automated fingerprint identification system.

²⁴ Nanavati, S. – Thieme, M. – Nanavati, R.: Biometrics. Identity Verification in a Networked World (2002), p. 147.

order. The potential for most types of privacy infringement in applications wherein the private sector is identifying individuals is much larger than in applications in which government is identifying customers.

On the basis of the seven aforementioned application-based classifications, it can be pointed out that the three primary roles an individual can occupy when interacting with an identification agent are: employee, citizen and consumer.²⁵

Employee identification refers to identification of an individual during the course of employment. **Citizen identification** refers to identification of an individual by a government body. **Consumer identification** refers to identification of an individual in the course of executing a transaction for goods or services.²⁶

Citizen-facing applications include criminal identification, citizen identification and surveillance. The defining element of citizen-facing applications is that a government body provides identification and enforces compliance with the biometric system's match decisions. Citizen identification includes identification for example the purposes of law enforcement or obtaining passport²⁷.

Employee-facing applications include PC/network security and physical access time and attendance. The defining element is that an institution provides identification and enforces compliance with a biometric system's match decisions.

Customer-facing applications include e-commerce and retail/ATM/point of sale. Also physical access/time and attendance can be included to customer-facing applications. The defining element of customer-facing applications is that a provider of goods or services provides identification of consumers and enforces compliance with the biometric system's match decisions. Customer-facing applications are normally based on verifying a claimed identity, not identification.²⁸

4. Societal issues of biometric identification

Biometric identification must be implemented with full awareness of various issues and concerns of privacy and societal perspective. We as individuals and citizens have the right to go about our lives anonymously from the eyes of the government and other organizations. We as a society highly value individual privacy, both physical and informational. Biometrics are perceived to impinge upon privacy, thus it is often viewed with suspicion.²⁹

According to a report from Rand Corporation on the use of biometrics, biometric identification raises three categories of societal concerns: religious, informational privacy and physical

²⁵ Nanavati, S. – Thieme, M. – Nanavati, R.: Biometrics. Identity Verification in a Networked World, p. 147.

²⁶ It is important to note that not every biometric usage falls within this categorization. For example a biometric door lock installed by an individual on his or her front door would be neither citizen, employee nor customer identification. This is because there is no external identification agent. However, every important biometric installation and deployment can be classified accordingly.

²⁷ The EU has deployed biometric passport. Finland has also started collecting biometric data to the permit of residence in January 2012.

²⁸ Nanavati, S. – Thieme, M. – Nanavati, R.: Biometrics. Identity Verification in a Networked World (2002), p. 157-208.

²⁹ Garfinkel, S: Database Nation: The Death of Privacy in the 21st Century (2000)

privacy.³⁰ Religious objections might arise from one or more religious groups because biometrics is considered as a “Mark of the Beast” based on the language in the New Testament’s Book of Revelation. It should be noted that although religious objections to biometrics may not be widespread, such objections need to be taken seriously because of respect.

Informational privacy concerns relate to three issues which are function creep, tracking and identity theft. Function creep is a term used to denote the process by which the use of information is slowly enlarged beyond the original purpose for which it was obtained.³¹ Function creep can be divided into four issues: Unnecessary collection of biometric information, unauthorized disclosure, unauthorized use of biometric information, and unauthorized collection of biometric information.³²

Tracking refers to the possibility of linking different transactions to build profiles. Because some biometric technologies can be used covertly, it is also possible that individuals could be tracked clandestinely. One such case occurred in 2001 during Super Bowl in Tampa Bay, Florida. Law enforcement authorities scanned the crowd using facial recognition technology in an attempt to identify criminals and terrorists.³³

Although the use of biometrics is expected to minimize identity theft, its benefits are still unclear because many biometric systems allow remote authentication. Furthermore, spoofing can also lead to identity theft.

Physical/personal privacy concerns centre around three issues as well. There is a percentage of the population for whom the use of biometric technology is inherently offensive, invasive, or disturbing. While some personal privacy fears may be derived from inchoate informational privacy concerns, this reaction is often attributable to cultural, religious or personal beliefs. Other individuals may feel that the implementation of a biometric system is an expression of mistrust and find the implicit mistrust insulting.

First is the issue of cleanliness and hygiene. Some user discomfort may occur when getting in contact with sensors which many other have been in contact with. This might cause worry of infection. The second issue is that of a potential harm ensuing from being scanned for a biometric measurement. Although biometric technologies are known to be fully safe, it is not difficult to perceive a potential harm. The third physical privacy issue is cultural: there might be stigmas attached to the capture of biometric information of certain kinds, e.g. fingerprints.

³⁰ Woodward, J.D, Jr – Webb, K – Newton, E – Bradley, M – Rubenson, D: Army Biometric Applications: Identifying and Addressing Sociocultural Concerns, p. 21-32. (2001), available at: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1237.pdf.

³¹ In Finland the chief of the police Mikko Paatero wants the police to have access to the passport registry for crime investigation purposes.

³² Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a Networked World (2002), p. 240-243.

³³ Woodward, J.D, Jr: Super Bowl Surveillance: Facing up to Biometrics, Rpt. IP-209 (Rand Publications, 2001), available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP209.pdf. See also Woodward, J.D, Jr: Biometrics – Facing up to Terrorism, Rpt. IP-218 (Rand Publications 2001), available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP218.pdf.

5. Closing notes

Reliable authorization and identification are becoming necessary for many everyday actions, be it boarding an aircraft, performing a financial transaction, or picking up a child from day care. Identification becomes a challenging task when it has automated with high accuracy and hence with low probability of break-ins and reliable non-repudiation. The user should not be able to deny having carried out the transaction and the use of biometrics should be as inconvenient as little as possible.

As the proverb says, for every problem there is a solution: Biometric technology has emerged as a viable solution for a range of applications where a person's identity must be verified or determined. No longer a science-fiction solution, biometrics are being deployed to solve security problems, to help companies generate revenues, and to protect personal information. As the sensors needed to acquire biometric features get cheaper and smarter, this technology has a greater potential than ever to change how we live, work, and do business.

Whilst recognising that such technologies can benefit the society, the principal question faced when using biometrics is to ensure that they are designed and used in full respect of fundamental rights. Therefore it needs to be said that when deciding to use biometric identifiers and choosing the most appropriate ones, due regard should be taken for the individual rights of the persons concerned, especially the right to data protection and privacy.

However biometrics technologies are still in their early stages and there are many challenges to be addressed. The most important challenge with biometrics is to ensure that biometrics are used intelligently and responsibly as the technology moves into mainstream. Also accuracy and the acceptance of the technology are a challenge. To gain a wider public acceptance, efforts aimed at educating people must be done. At the same time, current legal safeguards must be reviewed to ensure the privacy rights of individual. From this point of view, a question arises: Is biometrics the only real solution for today's problems in identification. This question still remains unanswered.

In the end one should note that with great power comes great responsibility. Unfortunately, not everyone understands this.

6. References:

The American Heritage Dictionary. Available at:
<http://www.ahdictionary.com/word/search.html?q=biometrics>

The Council of the EU. Glossary of Security Documents, Security Features and other related technical terms, available in English at: <http://prado.consilium.europa.eu/en/glossarypopup.html>

Garfinkel, S: Database Nation: The Death of Privacy in the 21st Century. Published by O'Reilly Media, Inc. 2000.

Nanavati, S – Thieme, M – Nanavati, R: Biometrics. Identity verification in a Networked World. Wiley Tech Brief Series. Published by John Wiley & Sons, Inc. (2002).

Sethi, I: "Biometrics. Overview and applications" in Katherine J. Strandberg and Daniela Stan Raicu (eds), Privacy and Technologies of Identity. A Cross-Disciplinary Conversation. Springer Science + Business Media, Inc. 2006.

Wayman, J.L.: Fundamentals of Biometric Technologies. Available at: http://www.engr.sjsu.edu/biometrics/publications_tech.html.

Woodward, J.D, Jr – Webb, K – Newton, E – Bradley, M – Rubenson, D: Army Biometric Applications: Identifying and Addressing Sociocultural Concerns, (2001). Available at: http://www.rand.org/content/dam/rand/pubs/monograph_reports/2007/MR1237.pdf.

Woodward, J.D, Jr: Super Bowl Surveillance: Facing up to Biometrics, Rpt. IP-209 (Rand Publications, 2001). Available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP209.pdf

Woodward, J.D, Jr: Biometrics – Facing up to Terrorism, Rpt. IP-218 (Rand Publications 2001). Available at: http://www.rand.org/content/dam/rand/pubs/issue_papers/2005/IP218.pdf.

World's biggest biometric ID scheme forges ahead. BBC News. Available at: <http://www.bbc.co.uk/news/world-asia-india-16979875>.

LEGITIMATE USE OF PERSONAL DATA IN CREDIT RISK ASSESSMENT

Lorena Donoso Abarca

Attorney, with a Master's in Informatics and Law
Assistant Professor on the Law Faculty of the University of Chile
Consultant to the Chilean Institute of Law and Technologies
lorena.donoso@gmail.com

Keywords: *Risk, Credit risk, Credit Risk Assessment, Scoring, Data protection*

Abstract: *The use of personal data involves an inherent conflict between personal interests, stemming from the need of individuals to control their own personal information, and the interests of society at large, associated with decision-making processes that must reflect the general needs of the citizenry. This paper seeks to clarify the conditions for the legitimate use of personal data in developing credit risk assessment criteria or credit "scoring," understood as elements that evaluate the ability and probability of a person being able to meet his or her credit obligations. The analysis entails answering the following questions: What is the legal status of the credit score that evaluates potential credit risk, in light of the regulations concerning personal data? Which personal data can be legitimately employed in developing risk criteria? Is it possible to respect the principles of the use of personal data in these systems? How can the rights of the holder of personal data be protected? In addition to answering these questions, we feel that the observations contained here are useful for both the market players and holders of personal data, as they deal with the implications that may impact the lives of the persons concerned and the needs associated with maintaining a macro-economic balance in society.*

1. The role of credit risk assessment in making decisions about credit

When speaking about credit risk assessments, we are referring to the way in which personal data of a financial nature is used¹ and analysed in an attempt to predict future payment behaviour. In other words, it deals with information about the financial situation of an identified or identifiable person that allows conclusions to be drawn with respect to his or her creditworthiness at any given moment. This information is essential to a lender who must make decisions about whether or not to extend credit to a particular person, and, if so, what the most appropriate credit terms are, given the level of risk the credit score indicates. In this regard, it has been said that a lender which uses quality information, explicit

¹ Article 2 of Law 19.628, on the protection of private life, states that the processing and use of personal data consists of any technical operation or set of operations or procedures, whether of an automated nature or not, that permit the collection, storage, recording, organising, production, selection, extraction, interconnection, dissociation, communication, cessation, transfer, transmission, or deletion of data of a personal nature or their use in any other way.

variables, and suitable methods (transparent algorithms) to produce accurate credit scores, provides a social benefit by offering better commercial terms to those applying for credit.

Players in the financial markets believe that risk predictors are needed to fulfil the aims associated with credit assessment. Their suitability has been recognised at both the national and international levels. The literature in this field indicates that in countries where there are credit bureaus, the possibility of obtaining credit increases considerably for individual persons and small- and medium-sized businesses, to the point of practically doubling their access to credit or, inversely, decreasing their barriers to credit by 50%.² However, questions arise as to exactly which data should legitimately be included in the algorithms, what is a reasonable way in which to evaluate this information, and how will the process be applied in each individual case.

In effect, diverse types of information are used to develop these risk indicators. The most accepted are those known as “qualified payment incidents,” which are delinquent payments on credit obligations. In addition, there is growing pressure to include information on the levels of indebtedness and “payments or services on contracted debt” paid on time and in the correct form. The reasoning behind the first data is evident – a poor payment history may predict future defaults. More controversial is the so-called “positive debt,” which refers to payment behaviour that fits the level of indebtedness. Defenders of this criterion hold that there is a systemic risk associated with over-indebtedness and that persons with appropriate debt levels and good track records with regard to payments deserve to receive a positive score and, in turn, better credit assessments and more favourable commercial credit terms. On the other hand, its detractors claim that it has neither been proven that this systemic risk exists, nor that this type of intrusion actually results in real benefits for the persons with respect to credit terms.

Another factor that has been considered in a credit score is the number of enquiries that third parties make with respect to particular persons. The inclusion of this information has been especially controversial in Chile. The data processing industry says that it adds useful predictive value, whereas its detractors maintain that this information is not generated by the holder of the personal data, but rather by third parties other than the holder of personal data. Moreover, they claim there is no assurance that this information is objective, and that it often involves injustices because the third parties may be acting out of malice that is, increasing the number of enquiries in order to damage the affected person’s ranking.

This paper shows that the apprehensions of the German Constitutional Court in 1983 are still in evidence today. The finding of the court was that personal data which may appear to be innocuous or irrelevant can result in arbitrary decisions and the stigmatisation of individuals through a process of systematisation and the submission of that data to procedures that result in the “profiling” of the persons. The profile is then translated into a score that determines whether the holder of the personal data is creditworthy or not. Moreover, this data often contains information on other aspects of the person, such as their consumer habits, their health care choices, and so on, depending on the degree of integration of the commercial system.

At this point, it should be evident that there are two fundamental aspects involved in developing credit risk assessments, or predictors of credit risk: a) the selection of data to be used in its calculation and; b) the calculation formula, which assigns factors and/or scores to each type of information. The statistical combination of these factors gives a greater or lesser predictive number or score with respect to a particular person: and in a majority of cases, the formula is the best guarded secret of its authors. From

² As an example see the case of Panama:

<http://www.iberpymeonline.org/CENPROMYPE0806/FINANCIAMIENTO/PANAMA.pdf> [enquiry: 15.02.2010].

our perspective on the use of personal data, we believe that it is critical to recognise the importance of these tools and to ensure that their construction is carried out in a manner that is consistent with the internationally accepted principles and norms for the legal protection of personal data, as we shall see below.

2. The legal nature of the predictors

In Chile, Law 19.628 defines personal data in the following terms: “those (data) pertaining to any information concerning identified or identifiable natural persons.”³ As one can see, legal persons are not included within the scope of this definition. This reflects the general trend. However, there are legislative bills currently under discussion that would extend the protection of personal data to legal persons, such as has occurred in Argentina. In order to do this, the legal person referred to must be identified or identifiable. In simple terms, this requirement is met to the extent that the data are capable of being attributed to a person, either directly or after performing certain relatively complex operations, whether they require technical support or not. In contrast, the regulation understands that statistical data, as opposed to personal data, are data that cannot be associated with an identified or identifiable holder of personal data, either in their origin or as a consequence of the way they are used.⁴

Clearly, credit scores are personal data, as they refer to an identified or identifiable person. Hence they are subject to regulations regarding the protection of personal data. The first consequence of this classification is that the person must have the possibility of accessing, rectifying, modifying, deleting, and/or blocking this information if and when it is the object of abusive treatment.

But this contention is not sufficient to clarify the legal nature of personal data. We must advance toward framing personal data in categories that are recognised by international classifications. This is important because being placed in a classification will allow personal data to be assigned specific levels of protection and rules for their use.

At least in Chile, by public data we mean that data which, in accordance with values rooted in our social conscience, are generally known by the public at large, or at least are easily accessible in public records, such as information in public directories. Owing to its nature, this data can generally be stored in databases that are available for public use, and the only requirement to access this information is that the person making the enquiry is doing so in accordance with the purpose for which it has been stored. We believe that the data on credit risk assessments do not belong in this category.

This being the case, we suggest that these data might be classified as *sensitive information or specially protected data*. By these terms, we mean that this data should only be accessible through the consent of the holder of the personal data or under special circumstances upheld by the law. If we consider that a primary reason to classify certain data as sensitive is that making this information available may lead to arbitrary decisions or involve questions directly impacting a person’s human dignity, or that it may be used to help construct a profile of a particular person or, as mentioned in the legislature, to obtain knowledge about the habits of a particular person, we reach the conclusion that such predictors can be considered sensitive data, inasmuch as these predictors try to foresee future behaviour through the systematization of experience and past behaviour, but only to the extent that they do not include other type of information, such as that generated based on enquiries from third parties or on the level of indebtedness of the person.

³ Article 2 letra f of Law 18.628

⁴ Art. 2 letra e of Law 19.628

This creates a paradox, in the sense that while the need to protect the data on credit risk assessments is clear, above all because its misuse can lead to arbitrary decisions with respect to this person, there is no category in current Chilean legislation that is appropriate for the inclusion of personal data, or at least there was none.

On the 25th of July a new law went into effect in Chile, Law 20.591. This new law modifies Article 9 of Law 19.628, concerning the protection of personal data and introduces the following clause: *“The production of any type of credit risk assessments or predictions that are not based solely on objective information related to payment defaults or protests of natural or legal persons are expressly prohibited. Violation of this prohibition shall require the immediate removal of said information by the party responsible for the database and adequate compensation for damages shall be awarded.”* This modification came about as the result of a parliamentary initiative triggered by a social event, namely that the parliamentarians noticed that “third party enquiries” were being used in the calculation of the credit ranking of particular individuals. In this regard, the law continues: *“Article 9° of Law N° 19.628 establishes that information collected or provided by sources that are accessible to the public must be accurate, current, and truthful with respect to the situation of the holder of the personal data, a legal prescription that is clearly altered when such data is used to produce a credit risk ranking or risk predictor, actions that are absolutely alien to the behaviour or the will of the holder of the data.”* In addition, the authors of the motion argued that information about the number of enquiries is not information that comes from a source that is accessible to the public and, therefore, access to such information requires the authorisation of the holder of the personal data. Thirdly, they pointed out that the use of this information leaves the holder of the data vulnerable, since it allows third parties to act in a malicious manner when conducting indiscriminate enquiries about a person with the sole aim of damaging their credit or reputation.

In synthesis, in their arguments the authors of this bill referred to three specific aspects, which are based on the application of the *principles of loyalty and legality* in the use of personal data with respect to instruments of credit risk assessment:

- a) Lack of quality of the information: inasmuch as it deals with non-factual information that does not originate from an action of the holder of the personal data, but rather is information generated due to the action of a third party, who is conducting an enquiry using the national identification number of the holder of the personal data.
- b) Lack of quality in the process: inasmuch as the enquiry deals with data pertaining to a national identification number,⁵ the information does not come from a database with free and open access to the public. Therefore, using this data requires the authorisation of the holder of the personal data, that is, the person whose national identification number is being consulted in the enquiry.
- c) Illegitimate application of consumer rights. In this regard, it is said that the inclusion of enquiries using the national identification number of a person hinders that person from performing legitimate actions, such as negotiating credit from a financial lender. Given the fact that each lending institution conducts credit risk assessments, this inadvertently affects the ranking of the person.

⁵ RUT (Rol Unico Tributario) refers to a person’s tax identification number.

Another important factor is a judicial ruling, court record N° 3937-2010, in the Court of Appeals of Santiago, which determined that the risk predictor of the respondent party (Equifax) violated the constitutional guarantees enshrined in numbers 2nd, 4th, and 26th of Article 19 of the Fundamental Charter. It maintained that “notwithstanding the awareness of the judges with regard to the effect of the ruling, it must be stated that in the opinion of the court obvious illegalities and arbitrary actions have been committed by the respondent party by means of producing the so-called “risk predictor” and making it available to the public. The court believes that the respondent party had neither legal authorisation nor factual reasons to justify carrying out said action and that this comprises a practice that should be ended in order to avoid the potential to unjustly damage the credit and reputation of persons.”

For our part, we understand that there is a great risk in legislating for the protection of data in this ruling, because in its eagerness to limit the use of predictors, it legitimises a new category of personal data: “appreciative personal data,” that is, data that is generated by a third party based on information pertaining to a person, where there the formula used by the third party is based two elements: a) the choice of the type of information to include in the basis for calculation, and b) the determination of the weight to give to each type of information chosen, as well as the rules (algorithms) for processing the data.

Until now, in Chile such appreciative data has not been subject to special regulation and, as the Court of Appeals noted in the case reviewed above, this type of data must be viewed as lacking a legal basis and, consequently, its use is illicit or at least lacking legitimacy. Looking at compared experience, in other settings we observe that special attention has been placed on the factual basis and transparency of the criteria used in developing these indicators, which, in any case, must respond to the *general principles* that govern the use of personal data. We will deal with this is the aspect below.

3. Legitimate conditions for using appreciative data to develop credit risk assessments

Developing an algorithm and applying it to a specific case is an operation involving the use of personal data. The way in which the legislation has embodied this concept is broad and recognises the complex character of the procedures for processing personal data, which includes from the phase of collecting the data up to the time of its communication, in which the affected party, the holder of the personal data, may or may not intervene.⁶ As a consequence, all of the information that is included in the process of developing the predictor is personal data and all the operations that are carried out in this regard are considered as using the data. Therefore, the information and the operations are subject to the general principles of the law and, more specifically, to those laws that govern these matters, namely:

- a) *The principle of purpose*: Article 9 of Chilean Law 19.628, sets forth the bases of the principle of purpose in dealing with personal data in the following terms: “*Personal data must only be used for the purposes for which they have been collected.*” According to this precept, the administrator of the database may only use data that do not come from sources that are accessible to the public within the framework of the purpose for which they were collected. This precept establishes the conditions for legitimate use of personal data in a prohibitive manner. Based on this principle, the generation of a credit score can only use information whose use is not limited by having been collected for a specific purpose different from the generation of the predictors. In Chile this limits the information to that

⁶ “Explanatory Notes on Agreement 108 of the Council of Europe.” N° 31.

provided voluntarily by the holder of the personal data and that coming from sources that are accessible to the public.

The principle of the quality of credit risk assessments: The principle of the quality with regard to the use of personal data constitutes the umbrella concept that covers all the consequences of the proper use of data, from the perspective of the quality of the processes and the systems employed in dealing with the legitimate use of data. As a result, this principle forms the basis of a regulation which must be subordinated to the application and interpretation of sectoral regulations. It dates back to the Baker Project (1969),⁷ which, in turn, dates back to the beginnings of the doctrine on the configuration and scope of *privacy* in an Anglo-Saxon context. Today this is embodied in the European Directive, 46/95, Article 6, which serves as a guide for our countries.⁸

The quality of data imposes duties associated with the suitability of the selected information and the legitimacy/legality of its use in this type of process, the suitability of the algorithms, the publicity of the use of personal data, the temporality of processing of personal data, and other relevant factors that we will discuss below. With regard to the first area, the conditions for using personal data and their suitability are related to their *pertinence and reasonability*, which means the data that are included must be *suitable, pertinent, and not excessive* with respect to the purposes for which they were collected and for which they are subsequently used.⁹ Thus, the *duty of deleting* data applies when the data do not comply with these conditions. Similarly, the *temporality of processing personal data* applies when the data are stored in a form that allows the interested parties to be identified for a period not greater than that necessary for the purposes for which the data were collected or for which they will later be used.

In Chile, this principle is set forth in Article 9 of Law 19.628, where it states, “*In all cases, the information must be accurate, current, and true with regard to the real situation of the holder of the personal data.*” What does this mean? For information to be *accurate*, it must be “*punctual, faithful, and thorough;*” for information to be *current*, means “*that it exists, is happening, or is being used during the time being referred to;*” and, finally, for information to be *true*, means that “*the judgement or proposition that cannot be rationally denied.*” While these qualities must be evaluated in each case, these concepts, which come from the Diccionario de la Real Academia Española de la Lengua, make it clear that to the extent that the personal situation of the holder of the data changes, the personal data contained in the registry must likewise be modified. As a result, the veracity and accuracy of the data are conditioned by the *present moment*, which means that any time data are processed, they must be modified in accordance with the situation of the holder of the personal data at that moment in time.

The use of personal data in credit risk assessments falls within the purview of the use of economic and financial data, which are susceptible to changes in legislation with regard to the suitability and pertinence of information, especially in the following terms:

- i. *With regard to consent:* If the data being used are economic, financial, or commercial in nature, the consent of the affected person is not required for their use. However, the holder of the personal data still has to be properly informed as to the activity in order to exercise his or her

⁷ Losano, Mario G., *et al*, *Libertad Informática y Leyes de Protection de Personal data*, Cuadernos y Debates, Número 21, Madrid, Spain, Centro de Estudios Constitucionales, 1989.

⁸ In this respect, European Directive 46/95, in Article 6 N° 1, letra d), states that the data must be *accurate* and, when necessary, *current*; all due measures must be taken for inaccurate and incomplete data, with regard to the ends for which they were collected or for which they were subsequently used, be *eliminated or rectified*.

⁹ Article 5 letra c, Agreement 108 of the Council of Europe of 1981 and Article 6 N° 1, letra c) Directive 46/95.

legal rights if they choose to do so. This likewise applies to data coming from sources that are accessible to the public. If variables or data of any other nature are to be used, the expressed consent of the holder of the data must be obtained.

- ii. *With regard to the temporality of processing personal data:* In comparative law, Convention 108¹⁰ recognises the principle of accuracy in Article 5 letter d), which requires that recorded data must be accurate and, if necessary, up-to-date, and letter e) of Article 5 imposes the duty of preservation, requiring that the data be stored in a form that allows for the identification of the interested parties for a period that does not exceed the time needed to accomplish the purposes for which the data was recorded.

Chilean legislation specifies that the only data that can be used in generating predictors is information based on fact and derived from the late payment history of the persons. To this must be added the information found within the timeframe in which the legislation authorises its use and/or communication.

Likewise, with respect to late payments, the law establishes that *the duty to modify applies* if the payment obligation is terminated or the creditor directly intervenes in some way. In such a case, within seven days after the obligation has been fulfilled, the creditor must notify the party responsible for the *records or databases accessible to the public*, who must report the protest or late payment in a timely manner so that it is duly entered into the public record. The holder of the personal data may call for the immediate modification and confirmation of fulfilment of the obligation to the creditor, as well as a written document establishing proof of payment. If the responsible parties fail to comply with their duties in this regard, legal action may be taken and compensation, as prescribed by law, shall be awarded.

As we can see, the expiration date of personal data sets a limit on the quality of personal data with regard to predictors. Law 19.628 states that expired data are “*that (data) which have lost their currency by the provision of the law, by reason of the fulfilment of the condition or the expiration of the assigned period for their validity or, if there is no express regulation, by the change of facts or circumstances.*” Consequently, personal data can accurately reflect the situation of their holder and represent an unpaid obligation, but their use may not be legitimate because the time period imposed on them by legislation has expired or the condition of their fulfilment has been met for the cessation of its use or communication. By way of example, in Chile it is not possible to communicate data on delinquencies with regard to basic services, such as water, electricity, gas, or the telephone.

The legal consequence of expiration dates of personal data is the obligation to eliminate or delete personal data from the databases. This is “*the destruction of data stored in records or databases, whatever the procedure employed for this,*” without requiring the holder’s request. Therefore, *the calculation formula of a risk predictor cannot include personal data that has become null and void*, either due to having met the conditions of its fulfilment, as is the case when the statute of limitations has passed, payment or another means of terminating the obligation has been made, or, as in the case of Law 19.628, the 5-year time period imposed by legislation for the communication of data related to late payments or protests has elapsed.

Now, after disclosing that it is not possible to include barred information in the formula of a predictor, the question which naturally arises is whether it is legitimate to include information related to late payments and protests when the data has not yet become null and void, but the 5-year time period set forth in legislation for the communication of data has expired; that is, when

¹⁰ Agreement N° 108 of the Council of Europe, January 28, 1981, for the protection of persons with respect to the automated use of data of a personal nature.

there is a difference between the statute of limitations and the 5-year period for communication of data. The answer to this question we find in Article 18 of Law 19.628, which states the following:

“In no case can the data referred to in the preceding Article, data related to an identified or identifiable person, be communicated after five years have passed since the respective obligation took effect.

Nor can data relating to said obligation continue to be communicated after the debt has been paid or has been terminated by other legal means.

However, data required by the courts of Justice to adjudicate pending lawsuits shall be communicated.”

As we can see, in this case, the legislation limits the legitimated use of these data. However, we understand that it is also illegitimate to communicate the results of the processes that have been carried out using such data. *This being the case, these data should not be included in the calculation formula of a predictor.* This notwithstanding, for data that were subject to protests and are in databases that are accessible to the public, the holder of that data must ensure that this data are eliminated at the time the payment is made, according to Article 19, clause 3.

We base this on the systemic application of the principle of loyalty and legality in the use of personal data and on the conceptualisation that establishes the law, both in terms of the use of personal data in general and the communication of data in particular.

Indeed, the law defines the communication of data in this way: *“to make personal data known in any way to persons other than the holder, whether they are specified or unspecified.”* We understand that *“in any way”* means that not only is direct communication of first-hand personal data proscribed, but any data which has been formulated based on the first-hand data is likewise proscribed.

- iii. **Reasonability:** Credit risk assessments follow technical norms based on the statistical sciences. The predictors are modelled on credit histories that are useful and effective for predicting future payment behaviour. In this regard, it is important to point out that, from the perspective of statistics, even though certain factors may be considered important for predictive purposes, Chilean legislation, in determining how the principle of reasonability relates to data concerned with past late payments, did not accept the opinion of the credit bureau, which maintained that an important factor for determining this risk is *“the quantity of enquiries from a third party.”* In this regard, the credit bureau argued that models based solely on indicators of previous payment behaviour show several disadvantages when compared to models that include other variables. Among the disadvantages are the following: a) they may punish economic sectors, such as the agricultural sector, joint ventures, or even politicians, who, as the media has reported on occasion, have been late in paying the debts incurred during their campaigns; b) they may hurt economic cycles and hence make it more difficult to rebound from an economic crisis; c) they may affect the dynamic flow of credit, because they require higher interest rates to be maintained during an economic recovery, thereby slowing down the recovery.¹¹
- iv. **Quality of process and prohibition of adopting automated decisions:** In general terms and, more specifically, in the European context it was found that the use of automated decision-making with regard to personal data did not produce quality results in evaluating personal traits, such as work performance, creditworthiness, reliability, behaviour, and so on. Once again we are not looking at

¹¹ See Hernández Corrales, Liliana & others, Desarrollo de una metodología propia de análisis de credit empresarial en una entidad financiera, in Estudios Gerenciales, Vol. 21 N° 97 Cal, Oct.-Dec., 2005 ISSN 0123-5923.

an absolute right. Thus, persons may be affected by an automated decision that was adopted within the framework of entering into or exercising a contract, provided that the request for the execution of the contract is presented by the credit applicant, who has been satisfied or has been extended appropriate measures to safeguard their legitimate interests, such as the possibility of defending their position or being authorised by laws that establish measures that guarantee their legitimate interest.¹²

Hence, in accordance with this requirement persons who design and apply risk assessments cannot impose decisions on third parties conducting enquiries, but rather must limit the information that they pass to third parties to risk indicators based on variables that are known and available to both the public and the holder of the personal data.

- b) *Publicity of the use of personal data*: This principle requires the adoption of measures needed to ensure a general awareness of the use of personal data, its purposes, the parties who are in charge of dealing with this data, and all the elements that generate the conditions for its correct identification and the effective exercise of the guarantees established in favour of the holders of personal data. However, we also need to distinguish whether the personal data are obtained directly from the holder or from a third party.¹³

In effect, the law in general requires that if the data are collected directly from the affected party, the affected party must be informed as to the party that is responsible for the use of the data, or, when appropriate, a representative thereof. In addition, the affected party must be informed of the purposes for which the data are being collected and any other information that is necessary to adequately safeguard the holder's rights, such as the recipients or classification of recipients of the data, whether or not a response is obligatory, and the consequences when there is no response when it was deemed obligatory. In contrast, if the data are collected from a third party, international standards¹⁴ require that the affected party be informed at the moment the data are recorded or, if one intends to communicate the data to a third party, at the moment of the first communication or earlier. In such a case the identity of the party responsible for the use of the data must be communicated or, when appropriate, a representative thereof, as well as the purpose of the use of data and any other information, such as the classification of the data, the recipients or classification of recipients of the data, the existence of rights of access and rectification of the data, and, to the extent that there are specific circumstances under which they have obtained the data, supplementary information is needed to ensure the data are processed in a manner that is fair to the party concerned.

As occurs in the case of the principle of consent, there are exceptions regarding the duty of information. Firstly, this right does not apply to the collection of data when the information about the affected party seriously hinders the fulfilment of the functions of control and verification of public administrations or when it affects national defense or public security or the prosecution of penal or administrative infractions. Likewise, the duty of information is not necessary if the content of the information is clear from the nature of the personal data that was requested or from the circumstances under which it was obtained.

¹² Article 15 Directive 46/95 EU.

¹³ An example in comparative law is found in Directive 46/95, of the Parliament and Council of the EU, in Articles 10 & 11.

¹⁴ By way of example, see Directive 46/95, Article 11 N° 1.

As far as we are concerned, the principle is manifested through the following elements: the ability to access information as to the identification of the natural person or legal person who is using the data; the specific data that were employed in creating the predictors and the weight that each factor contributes to the final result; the purpose of recording the data; the maintenance of the record; and providing information regarding third parties who have conducted enquiries about a particular person.

- c) *Security in the use of personal data of credit risk assessment*: In compliance with this principle, the party responsible for the use of personal data must apply the technical and organisational measures necessary to adequately safeguard the integrity, availability, or due access of personal data,¹⁵ at the levels of reasonability needed to guarantee a balance between the cost of the measure and the level of sensitivity of the data being used. These duties are the responsibility of the holder of the database of personal data, regardless of whether the processing is carried out by the holder or through a third party.

The Chilean legislation in this regard stipulates that the party responsible for the records or databases where personal data are stored must use due diligence in maintaining them and are liable for damages,¹⁶ covering both patrimonial and moral damage. Persons who work in the processing and use of personal data, in both public and private entities, are required to ensure the privacy of personal data that come from or have been collected from sources that are not accessible to the public, including the privacy of all other information related to the databases. This is an obligation that does not end when they are no longer actively working in that field.¹⁷

What we are interested in pertains to security in the processing and use of personal data, the operation of the algorithm in developing the risk index, how profiles of access to data are determined, the traceability of information, maintaining a systematic record of those persons who have consulted the predictors, indicating the day, hour, and response provided, and so on.

- d) *Principle of effective protection for the interested party*: This principle requires that all the necessary measures are in place to ensure that the interested parties can exercise their rights. It also entails establishing mechanisms that allow for complaints to be made to the corresponding oversight agencies with respect to the decisions made by the party in charge of the records or by third parties, which may affect or violate the rights of the interested parties. In this regard, legislation establishes that a catalogue of rights be granted to the holders of the data in order to provide for the proper safeguarding of their rights – the rights of access, rectification, and deletion.

In Chile, the holder of personal data is granted the rights as framed within the acronym “ARCO” (Access, Rectification, Cancellation [Deletion], and Opposition to the use of personal data). To this is added the right for the holder of personal data to demand compensation for damages caused by the

¹⁵ By way of example, see Article 17 Directive 46/95 CE, which states that in fulfilling this principle, one must “apply adequate technical measures and organisation for the protection of personal data against accidental or illicit destruction, accidental loss or alteration, dissemination or unauthorised access, in particular when the use includes the transmission of data in a network, and against any other illicit use of personal data.” Art. 7 Agreement 108, 1981 CE, states that “timely security measures to protect personal data that is recorded in automated archives against accidental or unauthorised destruction, accidental loss, as well as against unauthorised access, modification, or dissemination.”

¹⁶ Art. 11 Law 19628

¹⁷ Art. 7 Law 19628

illegitimate use of personal data. With respect to legal status, the right of access, the right of rectification, and the right of deletion are quite personal in nature and are exercised by the affected party or by their legal representative, when the affected party is incapable of doing so either due to a disability or due to being of an age that makes it impossible for them to personally exercise their rights.

Title II of Chilean law deals with the analysis of these rights. With regard to the right of access, which the law calls *the right of information*, a person has the right to demand that whoever is in charge of a database that deals publicly or privately with the use of personal data, information about data concerning that person, the origin or destination of that information, the purpose of storing that data, and the individualisation of the persons or entities to which the data are transmitted regularly.¹⁸ This right shall be demanded free of charge of the party responsible for the data files by the holder of the data, in accordance with the conditions established by law. Moreover, upon request the holder of the data must be provided with a copy of the record of his or her relevant personal data. The law establishes this as an inalienable, irrevocable right that cannot be limited by means of any act or convention.¹⁹

The *liable subject*, the party that is legally accountable for complying with this right, is the party that is responsible for the databases (in accordance with the classification adopted by the law). In the case of public administration it is the respective agency or entity that processes the data. If the personal data are in a database to which several entities have access, the holder may request information from any of them.²⁰

Finally, when there is *no timely pronouncement* (two working days) from the liable subject with regard to the request, or there is an *unjustified refusal*, the law establishes the writ of habeas data (access to personal data) as a mechanism of effective legal protection for the holder of the data. The competent court decides this based on the grounds for refusal, namely, whether *the refusal is based on a cause other than national security or national interests*. If the refusal stands, the holder of the data has the right to appeal to the judge in the district where the liable party resides and can request protection provided by the rights of information, modification, blocking, or deletion, as the case may be.²¹

We will not go into the exact procedures as established by law, but rather for our purposes, it will suffice to point out that if the judge rules in favour of the appeal, the court will set a reasonable time for the responsible party to comply with the ruling and may face a fine of between one and ten UTMs (monthly tax unit). If the information is not provided in a timely manner or there is a delay in carrying out the modification, as ordered by the court, the responsible party may be subject to a fine of from two to fifty UTMs. If the responsible party, which is in charge of the database, is a public agency, the court may sanction the head of the agency with a suspension of his or her duties for a period of from five to fifteen days.²² The law also includes the possibility that, together with the claim aimed at establishing the infraction, the affected party can request that action be taken against

¹⁸ Art. 12 inc. 1 Law 19628

¹⁹ Art. 13 Law 19628

²⁰ Art. 14 Law 19628

²¹ Art. 16 Law 19628

²² Art. 16 final clause

the natural person or legal person or public agency responsible for the database of personal data in order to obtain compensation for economic and moral damages suffered by the holder of the data, as a result of the misuse of the data. The compensation is determined by the court, which takes the circumstances of the case and the gravity of the matter into account. This action will follow summary proceedings, with the evidence being duly evaluated and a ruling rendered by the court. Other legal processes arising from infractions not covered in Article 16 (violations of the right of information, modification, blocking, or deletion) and Article 19 (deletion or blocking of personal data related to economic, financial, bank, or commercial obligations) will also follow summary proceedings.²³

This action is taken notwithstanding the duty of the responsible party to eliminate, modify, or block the data in accordance with the request of the holder of the data or, if appropriate, as ordered by the court and as established in Article 173 of the Code of Civil Procedure. Finally, it is important to point out that the law directs the judge to take off measures deemed necessary to enforce the protection of these rights.

4. Conclusions: On the legality of the use of information emanating from third parties

In our opinion, Chilean legislation prior to the enactment of Law 20591 adequately embodied the principle of quality of data and contained regulations that were fully applicable to such matters. Therefore, the modifications of legislation dealt with in this analysis were, to our minds, unnecessary.

In effect, Article 6 of Law 19.628 already establishes that for the use of personal data to be legitimate, the following requirements must be met: a) There must be legal grounds for the storage of personal data: Law 19.628 already authorises the processing, storage, and use of personal data; b) The data must be *true and valid at all times*, in such a way that the information is accurate, current and true with regard to the situation of the holder of the data. Thus, once any of the data are expired, erroneous, inaccurate, mistaken or incomplete, the regulation has been contravened.

The corrective measures that the law provides with respect to inaccurate data are set forth in the *duty of rectification*,²⁴ which states that data must be modified whenever they are inaccurate or erroneous, and in the duty of *elimination or deletion*, which states that data must be deleted when they have expired or become obsolete and, in such a case the party responsible for the use of the data must promptly notify this fact to anyone who has reported the data.²⁵ If it is not possible to determine the persons to whom the information has been communicated, a notice must be published that can provide general knowledge to those who use the information of the database. Finally, the party responsible for the use of the data, has the duty to *block* the data, but not delete or eliminate them, when their veracity is dubious or their use is improper. There are no sectoral regulations which establish exception to the modification, deletion, or blockage of stored personal data.

We realize that the new legislation was intended to reinforce and strengthen these principles and rights. The intention was to establish prohibitive regulations in order to prevent that the rights of a person could be limited by contractual agreements, and to ensure that only factual and current information is

²³ Art. 23 Law 19628

²⁴ Arts. 6 & 12 clause 2 Law 19628

²⁵ Art. 12 Law 19628

used to develop credit scores of financial risk. To this end, the use of historical data for the purposes of predicting future risk may not be legitimised by contractual means. This is emphasised in Article 18, which states:

“In no case may the data referred to in the previous Article, related to an identified or identifiable person, be communicated after five years have elapsed from the time the respective obligation fell due.

Nor may data related to the said obligation continue to be communicated after the obligation has been paid or has been discharged by other legal means.

However, information which is required for pending lawsuits may be communicated to the Courts of Justice.”

Consequently, by stipulating “*in no case*,” an exception is being established with respect to the right of a person to consent to the use of personal data concerning her or him, which is already recognised in general by Law 19.628.

This interpretation is consistent with the legal nature of Law 19.628, as this is the regulation that develops a fundamental right, guaranteed by the Constitution, which imposes a limitation on those regulations that restrict the rights in question.

In response to the previous legal reasoning, we understand that when these regulations are contravened, the following penalties are applicable under Article 16: (1) the elimination of historical information; (2) fines of from 1 to 10 UTM;²⁶ (3) fines of from 10 to 50 UTM per infraction of Articles 17 & 18; and (4), in addition, compensation for the respective economic and moral damages.

In this regard, when compared with laws in Spain, where the standards of protection of information are the highest on the planet, the National High Court, in its finding 18th January, 2006²⁷ maintained that “... and there is no doubt that the penal provisions of the LOPD (Data Protection Act) applies to the party which supplies that data to the party responsible for maintaining the database, as the party supplying the data is the party which really knows the actual credit situation, as to whether or not the terms have been met and what time such actions took place. Ultimately, it is the party which knows the latest situation as to the solvency of the affected party. And whenever there is a modification of that situation, it must inform the party responsible for the database, in order for the database to reflect the truth as to the current situation of the affected party.” Thus, it is clear that, with regard to the quality of the use of personal data, the party that is processing and using the data would find it very difficult to hide the fact that it is conducting contemporaneous enquiries with respect to the same person.

²⁶ The UTM (Unidad Tributaria Mensual) is an economic indicator used to update the monetary situation.

²⁷ Criteria endorsed in Resolution of File N°: E/01147/2006, Spanish Agency of Personal Data Protection, online at: http://www.agpd.es/portalweb/resoluciones/archivo_actuaciones/archivo_actuaciones_2008/common/pdfs/E-01147-2006_Resolucion-de-fecha-29-09-2008_Art-ii-culo-4.3-LOPD.pdf [enquiry: 15.02.2010].

THE PRODUCTION OF IDEAL CITIZENS IN THE DIGITAL AGENDA FOR EUROPE: A NARRATIVE PERSPECTIVE

Minna Saariketo

Doctoral student at the University of Tampere,
School of Communication, Media and Theatre.
minna.saariketo@uta.fi

Keywords: *Agency, strategy, technotopia, narrative analysis, Digital Agenda for Europe.*

Extended Abstract

What kind of a technological future is constructed by narrative means in the Digital Agenda for Europe? Who are the actors in the story and what are their roles in the plot? What roles are offered to citizens and which skills are emphasized?

Answers to these questions were sought through a narrative analysis of the Digital Agenda for Europe (DAE), published by the European Commission in 2010. The DAE is part of the Europe 2020 Initiative, the EU's growth strategy in this decade, and it is a continuation for European information society strategies such as eEurope 2002 – An information society for all (2000) and i2010 – A European Information Society for growth and employment (2005). The objective of the DAE is “to chart a course to maximise the social and economic potential of ICT” and “to make Europe a powerhouse of smart, sustainable and inclusive growth on the global stage”. Successful delivery of the Agenda is believed to “spur innovation, economic growth and improvements in daily life for both citizens and businesses”.

The Agency was chosen as the central concept of this case study because it enables an analysis of how the European Union participates in defining the actor roles of its citizens. Narrative analysis was used as methodology because narrative is a linguistic form uniquely suited for displaying human existence as situated action, and narrative descriptions exhibit human activity as purposeful engagement in the world.

The vision in the DAE is an example of a contemporary political narrative that is told to keep up faith in a better future. According to the story analysis inspired by Vladimir Propp's morphology of the folktale (1973), Algirdas Julien Greimas' actant model (1980) and Mieke Bal's theory of narrative (1985), the DAE is a technotopian narrative that adheres to an old progress myth, simply positing that new technologies will benefit society socially and economically and improve the quality of life of all individuals with access. The technological future outlined in the Agenda offers quicker and easier access to consumer markets for citizens, better profits for companies and it guarantees that Europe's economy can compete better with the United States and Asia. The main roles cast for citizens are either the role of workers in the ICT sector or the role of consumers. This casting is due to economic aims: citizens are needed in maximizing the economic potential of ICT to ensure the EU's economic growth and competitiveness. The technotopian plot in the DAE is part of the competition society politics, and the key words for future society in the DAE are innovation, creativity, entrepreneurship and competitiveness.

Curiously, the DAE can be read as a plot in itself. The narrative analysis shows that the main character in the story is the European Commission. It is the actor mentioned most often and most regularly. The Commission plays the key role in naming the problems, defining the solutions and putting into effect the action plan. A central and undeclared objective of the DAE seems to be to give the Commission and EU a central role with issues that they have a limited influence on. In other words, the DAE aims at giving the Commission a key role in shaping the European future to reinforce its authority and prestige.

The analysis emphasizes the need to find and create alternative stories which are not dominated by economy, competition and technological development as uncontested facts that citizens and the society have to adapt to.

[My presentation in the KnowRight 2012 conference has been developed into a referee-article that was published in Finnish by the national journal *Hallinnon Tutkimus* 4/2013 (Administrative Studies Journal) with the title “Tulevaisuuden ihannetoimijan tarinallinen tuottaminen Euroopan digitaalistrategiassa” (Producing the ideal actor according to the Digital Agenda for Europe: a narrative perspective). An article in English for an international refereed journal is under preparation.]

INDEX OF AUTHORS

Aarnio, Reijo	25
Abarca, Lorena Donoso	335
Ampuja, Marko	95
Anttinen, Terhi	305
Böszörményi, Janos	33, 171
Brunet, Laura Nahabetián	147
Bruun, Niklas	189
Filippi, Primavera De	233
Galindo, Fernando	289
Gracz, Katarzyna	233
Herler, Brita Kristina	217
Hötzendorfer, Walter	33, 113, 171
Iglesias, Romina Garrido	159
Jakob, Georg	239
Kiskis, Mindaugas	197
Kloza, Dariusz	119
Koivisto, Juha	95
Korhonen, Rauno	279
Korja, Juhani	323
Mincke, Wolfgang	265
Nieminen, Hannu	169
Ojala, Anu	179
Pöysti, Tuomas	41
Reyes, Patricia	87
Rizzi, Mariagrazia	239
Ronkainen, Anna	209
Saarenpää, Ahti	19, 97
Saariketo, Minna	349
Schweighofer, Erich	113, 171
Streng, Alfred	247