DATA PROTECTION AND INTELLECTUAL PROPERTY IN THE EU AND TURKEY

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF SOCIAL SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

ÖZLEM TOĞUZ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF EUROPEAN STUDIES

MAY 2010

Approval of the Graduate School of Social Sciences

_____

Prof. Dr. Sencer Ayata
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.

_____

Assist. Prof. Dr. Galip Yalman
Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

_____

Assist. Prof. Dr. Gamze Aşçıoğlu – Öz
Supervisor

Examining Committee Members

Assist. Prof. Dr. Gamze Aşçıoğlu-Öz	(METU, ADM)	_____
Assoc. Prof. Dr. Erkan Erdil	(METU, ECON)	_____
Dr. Uğur Yalçıner	(METU, STPRC)	_____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name : Özlem Toğuz

Signature :

ABSTRACT

DATA PROTECTION AND INTELLECTUAL PROPERTY IN THE EU AND TURKEY

Toğuz, Özlem
M.S, Department of European Studies
Supervisor: Assist. Prof. Dr. Gamze Aşçıoğlu-Öz
May 2010, 114 pages

This research had two main purposes. Firstly it aimed at showing the regulatory framework of both data protection and intellectual property in the European Union and thus making the privacy complications of Digital Rights Managements systems clear in the developed world. This research also aimed at disclosing the complications of employment of DRMs systems in developing countries. To that end Turkey's copyright framework has been reviewed. It was found out that DRMs systems employed in Turkey went beyond the scope of Turkish Copyright Legislation and restricted also legitimate acts which fall within the scope of fair use. DRMs also have hindered development since it restricted availability of educational and cultural works.

The review of Turkey's Data Protection regime disclosed that the most important reason behind the non adoption of the draft law was related to the legislators' confusion of first pillar and third pillar data protection. It was concluded that Turkey lacked a data protection policy and the lack of such a policy led to the surveillance of the people to such a degree that almost no private space is left for them.

The main finding of the research was that Turkey has been one of the best markets for the employment of DRMs with its current copyright regime and lack of data protection rules. The research concluded with proposals of action concerning data protection and DRMs.

Key Words: Data Protection, Intellectual Property, Turkey, European Union

ÖZ

AVRUPA BİRLİĞİ VE TÜRKİYE'DE
KİŞİSEL VERİLERİN KORUNMASI VE FİKRİ MÜLKİYET

Toğuz, Özlem
Yüksek Lisans, Avrupa Çalışmaları Bölümü
Tez Yöneticisi: Yrd. Doç. Dr. Gamze Aşçıoğlu-Öz
Mayıs 2010, 114 sayfa

Bu araştırmanın iki ana amacı bulunmaktadır. İlk olarak bu tez, Avrupa Birliği'nin kişisel verilerin korunması ve fikri mülkiyet ile ilgili yasal çerçevelerini inceleyerek, gelişmiş ülkelerde dijital hak yönetimi sistemlerinin mahremiyetin korunması konusunda yarattığı sıkıntıları ortaya koymayı amaçlamıştır. Bu araştırma ayrıca, dijital hak yönetimi sistemlerinin gelişmekte olan ülkeler açısından yarattığı sorunları da ortaya çıkarmayı hedeflemiştir. Bu doğrultuda Türkiye'nin fikri mülkiyet rejimi incelenmiştir. İnceleme, Türkiye'de kullanılan dijital hak yönetimi sistemlerinin fikri mülkiyet mevzuatının kapsamını aştığını ve adil kullanım hakkı kapsamına giren eylemlerin de sınırlandığını ortaya koymuştur. Dijital hak yönetim sistemlerinin ayrıca eğitim araçlarına ve kültürel çalışmalara erişimi kısıtlayarak gelişimi engellediği anlaşılmıştır.

Türkiye'nin kişisel verilerin güveliği rejiminin araştırılması, taslak kanunun imzalanmamasının arkasındaki temel nedeninin yasama organının birinci ve üçüncü sütun kişisel veri güvenliği hususlarını birbiri ile karıştırması ile ilgili olduğunu göstermiştir. Türkiye'nin bir kişisel veri güvenliği politikası bulunmadığı ve bu gibi bir politika eksikliği nedeni ile kişilerin nerede ise kendilerine özel alan bırakmayacak şekilde izlenmelerinin mümkün olduğu sonucuna ulaşılmıştır.

Bu araştırmanın ana bulgusu, Türkiye'nin kişisel veri güvenliğine yönelik kurallardan yoksun oluşu ve mevcut fikri mülkiyet rejimi ile dijital hak yönetimi sistemlerinin uygulanması açısından en iyi piyasalardan biri olduğudur. Araştırma, dijital hak yönetimi ve kişisel veri güvenliği ile ilgili aksiyon önerileri ile son bulmaktadır.

Anahtar Kelimeler : Kişisel Verilerin Korunması, Fikri Mülkiyet, Türkiye, Avrupa Birliği

To the memory of my deceased uncle Ahmet Toğuz…

ACKNOWLEDGEMENTS

I would like to thank my advisor Assist. Prof. Dr. Gamze Aşçıoğlu –Öz for her to the point comments which always have put me back on track whenever I lost my way while writing this thesis.

I would also like to express sincere gratitude to the other members of my examining committee: I would have more difficult time in reaching out a final draft if Assoc. Prof. Dr. Erkan Erdil did not show me the light at the end of the tunnel and Dr. Uğur Yalçıner did not encourage me to continue walking till the end. It has been a great journey and adventure thanks to the guidance and kindness of my advisor and the other members of my examining committee.

My special thanks to my inner child complex Dea, and my shadow self Aurora for not sabotaging my study and allowing me finish what I have started to do. Thanks to my true self for integrating different parts of my psyche and thus making me become a self-realized unity during the time of writing this thesis, thanks for the joys and agony of the inner journey which finally led to integration.

I would like to express my gratitude to my father, Mahmut Toğuz, who showered me with the light of his wisdom during all difficult times, without the generous light of his wisdom, I would simply get lost in the walk of life.

And finally thanks to my amazing partner Ivan Bakij for sharing his great soul with me and for his constant and persistent support.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AACS	Advanced Access Content System
CD	Compact Disc, Copyright Directive
CSS	Content Scrambling System
CPCM	Content Protection and Copy Management
GSM	Global System for Mobile Communications
DG	Directorate General
DMCA	Digital Millennium Copyright Act
DPA	Data Protection Authority
DPD	Data Protection Directive
DRM	Digital Rights Management
DRMs	Digital Rights Management Systems
DVB	Digital Video Broadcasting
DPEC	Data Protection and Electronic Communication
EC	European Community
ECJ	European Court of Justice
ECHR	European Court of Human Rights
EFF	Electronic Frontier Foundation
EU	European Union
HLG	High Level Group
IP	Intellectual Property
ISP	Internet Service Provider

IT	Information Technologies
RMI	Rights Management Information
TPM	Technological Protection Measure
WIPO	World Intellectual Property Organization
WP	Working Party

CHAPTER 1

INTRODUCTION

A life is considered more private when it is either searched or monitored less. For example when someone walks on the streets he is monitored by other people and his life can be searched if he has recorded it in letters or diaries. The level of monitoring and searching of other people's life is higher in more traditional and less developed countries. In such countries, especially in small towns almost everybody monitors the life of others. They monitor what others do, how they do it, when they do it etc. Thus in more traditional societies the lives of people are more public and less private. The monitoring of other peoples life makes social control easier.

Up to the digital age what made privacy possible in the traditional societies of developing countries were the walls of the houses that separated people from each other. Since those walls were also where the properties of one began, it was only possible to search inside of those walls under certain circumstances by the police.

However developments in technology have changed the balance of privacy that existed in the analogue world. It has become much easier to monitor the lives of people due to developments in the technology. And this change in the balance required laws to rebalance privacy.

First of all this thesis aims at finding out how in developed world and especially in the EU the gap of privacy created by the digitalization of the world has been filled. It further questions whether the criticisms raised

against the data protection policies of the EU are also applicable for the developing countries and Turkey in special.

The main question of the thesis is whether the application of DRMs has equal consequences in the developed world and developing countries. To this end after examining EU data protection policy, this thesis reviews the IP policy of EU, tries to give concrete answers to the privacy complications created by the employment of DRMs in the EU and further questions the implications of DRMs usage in Turkey. Since in the digital world, the enjoyment of rights to privacy and data protection have become highly linked to the digital enforcement of intellectual property rights and basically copyright.

To provide answers to the above stated question this thesis begins, in Chapter II, by providing information on the global developments on digital rights management systems. Chapter III summarizes EU's Data Protection Laws and Institutions and further explains the basic data protection principles and concepts. Chapter IV focuses on EU's Intellectual Property Policy and Intellectual Property Laws to give an insight on the approach of EU to Intellectual Property issues and further demonstrates the impact of EU's Data Protection Laws on Copyright and thus shows the interaction of Data Protection and Intellectual Property in the EU.

After examining both data protection and intellectual property faces of the coin conserning the EU and the interaction of these two "knowledge" related sets of legal rules in the EU, this thesis, in Chapter V tries to find out how these knowledge related issues regulated in Turkey. To this end the thesis provides the current situation of Turkey when data protection and intellectual property rights are concerned. After providing the legislative background and lack thereof, Chapter V shows the implications of DRMs

usage in the developing countries like Turkey and also emphasizes the importance of privacy laws in developing countries.

The research shows that certain policies that may seem luxurious in the developed world may be of crucial importance in the traditional societies of the developed world and different policies and sets of legal rules that may be considered highly necessary in the developed world may hinder development in the developing countries.

To be more precise, the first basic argument of this thesis is that while data protection rules may be considered to be unnecessary in the developed countries whose societies have a long privacy tradition and culture, in the digital world, where all technology is imported by the developing countries and where there is not a privacy tradition, the non existence of necessary legal framework to protect privacy may cause fatal consequences in terms of basic human rights. In other words what can be considered luxurious in EU may be of crucial importance for Turkey.

Secondly this thesis argues that in the lack of data protection rules certain technologies that protect copyright may not only hinder privacy they may also be detrimental for the development of countries. This research shows how DRMs not only hinder privacy but also development in Turkey where the only DRMs related concern in the developed world may just be limited to privacy.

Finally this thesis concludes with recommendations of action concerning data protection and digital rights management in Turkey.

CHAPTER 2

DIGITAL RIGHTS MANAGEMENT SYSTEMS

2.1. Technological Protection Measures

Technological protection measures are technologies created to protect copyrighted works from being copied and in the 1990s; copyright industries were willing to gain legal support for these technologies[1].

TPMs and digital rights management systems have been criticized by activists and academicians in terms of privacy[2]. Ian Kerr and Jane Bailey, leaders of the privacy Project, have made emphasis on the social consequences of employment of digital rights management (DRM)[3]. The authors were concerned that the use of digital rights management might hinder rights to data protection and freedom of expression[4].

These concerns about TPMs were justified over Sony BMG rootkit software scandal in late 2005[5]. Sony sold CDs containing digital rights management systems, which breached the privacy and security of consumers. [6].

[1] Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007, p:158.

[2] ibid, p:171.

[3] Kerr, I. and Bailey J., The Implications of Digital Rights Management for Privacy and Freedom of Expression, Journal of Information, Communication and Ethics in Society, 2004, 2, p:87-97.

[4] Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007, p:171.

[5] ibid, p:172.

[6] Ibid, p:172.

2.2. DRMs in General

In general terms, DRM is a type of technological protection that follows the subject of copyright wherever it may go[7].

Digital rights management systems is a term used to express a wide range of technologies that have the capacity to monitor, regulate, and/or price each use of a video, audio, photo, print or any other media content[8]. Since DRM is an umbrella term, it is used by professionals of different disciplines in different meanings[9]. DRM covers a wide range of technologies employed by publishers, individuals, hardware manufacturers or other copyright holders for the imposition of limitations or restrictions on the usage or copying of digital content and devices. DRM usually is a system comprising of a technological tool and usage policy designed for the secure management of access to digital information and the secure use of the same[10]. DRM can also be defined as an electronic security guard that monitors and controls access and use of copyrighted works.

DRM often uses encryption technology to protect works.[11] DRM is different from simple copy-control mechanisms or password protections, since it automatically creates and enforces complicated licensing terms in relation to copyright works[12]. For example, if a user is allowed to read an article once for fee under a DRM license; the DRM system might automatically delete

[7] Cameron A., Digital Rights Management: Where Copyright and Privacy Collide, Canadian Privacy Law Review, 2004, p:3.

[8] Einhorn, Michael A., Canadian Quandary: Digital Rights Management, Access Protection, and Free Markets, the Progress and Freedom Foundation, Release 13.12. May 2006, p:2.

[9] CIPPIC Report, Digital Rights Management Technologies and Consumer Privacy, An Assessment of DRM Applications under Canadian Laws, September 2007, p:3.

[10] İbid, p:4.

[11] İbid, p:3.

[12] İbid, p:4.

the article when the user attempts to copy it.[13] Using DRM systems is advantageous for the copyright holders because instead of applying to courts the jurisdiction of which is limited by geography, they can automatically write and enforce their own rules in licenses with each individual[14].

However beyond just inhibiting violations, copyright holders desire to use DRM to transfer content. DRM enables owners to monitor or record every use of a work.[15].

The "rules of use" enforced by DRM are called "usage policies". Such policies might include rules like "do not copy," "play for a week," or "install only on this hardware."[16] These usage policies managed by DRM can be elaborate and go far beyond just access and copy-control. For example, the DRM system may also function as a payment system which deals with payments and information related to the payments for individual licensed rights under the usage policy [17].

2.2.1 Digital Rights Management and Films

- **The Content Scrambling System**

The Content Scrambling System (CSS) was one of the antecedent DRM systems.[18]. The system was developed by the DVD Consortium.[19] It was a tool that compelled hardware corporations to develop systems which didn't accommodate certain components that allow a movie to be copied

[13] İbid, p:4.

[14] ibid, p:4.

[15] ibid, p:4.

[16] ibid, p:5.

[17] ibid, p:5.

[18] McGuigan, B., "What is DRM", http://www.wisegeek.com/what-is-drm.htm, last checked at 26.10.2009.

[19] An international organization known also as the DVD Forum, established by the following companies: Hitachi Ltd, Panasonic Corporation, Mitsubishi Electric, Pioneer Corporation, Royal Philips Electronics N.V., Sony Corporation, Thomson, Time Warner Inc., Toshiba Corporation, Victor Company of Japan, Ltd.

easily [20]. The DVD Consortium was able to impose hardware policy for the DVD industry by issuing the encryption key for CSS only to hardware corporations that admitted not to accommodate certain components[21].

- **The Protected Media Path**

Microsoft's Windows Vista[22] encompasses a DRM system, namely the Protected Media Path (PVP). The system targets to impede DRM-contained media from functioning when illegitimate software is running. For the purpose of making illegal recordings harder, PVP encrypts information while transferring to the monitor.[23]

In 2006, a campaign named Badvista Campaign was initiated. The campaign championed freedom for computer users and confronted Windows Vista on this ground.[24]

- **The Advanced Access Content System**

Advanced Access Content System (AACS) is a DRM system for HD DVD [25] and Blue-Ray Discs[26]. A consortium that is comprised of Disney, Intel, Microsoft, Panasonic, Warner Brothers, IBM, Toshiba, Sony has developed the system[27]. The AACS can be considered as the successor of the CSS.

- **The Broadcast Flag**

[20] McGuigan, B., "What is DRM", http://www.wisegeek.com/what-is-drm.htm, last checked on 20.10.2009.

[21] ibid.

[22] A line of operating systems developed by Microsoft.

[23] "DRM and Film", http://www.bigurlpro.info/DRM-film.html, last checked on 20.10.2009.

[24]Badvista, "FSF launches campaign against Microsoft Vista", Press Release, http://badvista.fsf.org/blog/launch-press-release, last checked on 20.10.2009.

[25] Short for High-Definition/Density DVD.

[26] An optical disc storage medium designed to supersede the standard DVD format.

[27] DRM and Film", http://www.bigurlpro.info/DRM-film.html, last checked on 20.10.2009.

In 2001, Fox Broadcasting has created the broadcast flag. The system was supported by the MPAA[28] and the FCC[2930].

The Broadcast Flag was adopted by the Digital Video Broadcasting Project (DVB). DVB was a consortium which aimed at developing new digital TV standards. 250 broadcasters, manufactures, network operators, software developers, and regulatory bodies from about 35 countries involved in DVB[31].

The Content Protection and Copy Management (DVB-CPCM) was the descendant and an updated alternative for the broadcast flag. The technical specification DVB-CPCM was submitted to European governments in March 2007[32]. According to the commentators the CPCM system also intended to control use of copyrighted material by the end-user, at the direction set forth by the copyright holders[33]. The CPCM has been submitted to the European Telecommunications Standards Institute in 2008[34].

2.2.2. Digital Rights Management and Music

DRM is used by online music stores to restrain operation of copyrighted music bought and downloaded online[35]. Below are different online music shops and the DRM systems employed by them:

[28] The Motion Picture Producers and Distributors of America, a United States non-profit business and trade association to advance the business interests of movie studios.

[29] The Federal Communications Commission.

[30] DRM and Film", http://www.bigurlpro.info/DRM-film.html, last checked on 20.10.2009.

[31] ibid.

[32] ibid.

[33] ibid.

[34] "DRM and Film", http://www.bigurlpro.info/DRM-film.html, last checked on 20.10.2009.

[35] "Internet Music", http://www.bigurlpro.info/internet-music.html, last checked on 20.10.2009.

- Apple Inc., employed a DRM system called FairPlay in its products and services, such as iPod, iTunes and iTunes Store. [36]. FairPlay DRM allowed copyrighted works to be played on authorized computers and at most five computers may be authorized at the same time[37]. Purchasers could burn (copy) their music files. How many times a file can be burned was not restricted but a certain playlist could not be burnt more than seven times.[38] Since Apple refused to license its technology, songs purchased from iTunes Store would only play on Apple's iPod media player. And the users could only buy DRM protected songs adoptable to iPod[39]. On January 6, 2009 Apple communicated that iTunes music will be ready for use totally DRM free as of January 2009. [40]
- Napster music store employed a DRM system which was based on subscription for purchases[41]. The DRM functioned thus: Users of the subscription based service could download an unlimited amount of music during the period of subscription. The music downloaded was transcoded to Windows Media Audio.[42] When the subscription period lapsed, all the music downloaded was becoming unplayable and the users had to renew their subscription[43].
- Sony conducted a service under the name "Connect" which worked only using Sony's OpenMG DRM technology[44]. Music downloaded from this service could be played on computers which use Microsoft

[36] Rayna T., Striukova L., Digital Rights Management: White Knight or Trojan Horse, Discussion Paper, Department of Economics University of Bristol, 2007, p: 4.

[37] ibid, p: 4.

[38] Rayna T., Striukova L., Privacy or Piracy, Why Choose?, Two Solutions to the Use of Digital Rights Management and Protection of Personal İnformation, International Journal of Intellectual Property Management, Vol 2, No:3, pp:240-252, 2008.

[39] Rayna T., Striukova L., Digital Rights Management: White Knight or Trojan Horse, Discussion Paper, Department of Economics University of Bristol, 2007, p: 4.

[40] "Internet Music", http://www.bigurlpro.info/internet-music.html, last checked on 20.10.2009.

[41] ibid.

[42] ibid.

[43] ibid.

[44] ibid.

Windows or Sony hardware. Playstation Portable and some Sony Ericsson phones were also compatible with the DRM[45].

- As a consequence of consumer dissatisfaction over complicated DRM systems, leading labels started to give up using DRM in music. Apple's CEO Steve Jobs in an open letter titled "Thoughts on Music" has invited the music industry to sell DRM-free online music[46].

2.2.3. Digital Rights Management and E-books

DRM systems are also used to limit copying, printing, and/or sharing of e-books[47].

Adobe Acrobat and Microsoft Reader are two of the most popular software programs to view e-books[48]. There is scarcely any difference between the approaches these two software programs use on e-book content protection[49].

In Microsoft Reader, its own DRM software is embedded[50]. DRM systems employ three different layers of access control for different types of e-books[51]. Sealed e-books only inhibit the document from being revised thus the user cannot change the book. Sealed e-books are the less stringent forms

[45] ibid.

[46] ibid.

[47] "Internet Music", http://www.bigurlpro.info/internet-music.html, last checked on 20.10.2009.

[48]Coyle,K.,"The Technology of Rights: Digital Rights Management",(PDF). http://www.kcoyle.net/drm_basics.pdf., 19.11.2003, last checked on 26.10.2009.

[49] "Internet Music", http://www.bigurlpro.info/internet-music.html, last checked on 20.10.2009.

[50] ibid.

[51] ibid.

of e-books in terms of DRM restrictions.[52] Inscribed e-books include a more stringent form of restriction[53]. Microsoft Reader includes a digital ID pin which results in the identification of the user of the e-book after the e-book is purchased and downloaded[54]. Different e-book softwares include coincidental DRM arrangements. Ereader which is employed by Palm Digital Media with the purpose of intimidating circulation of the books attaches the credit card information of the customer to the e-book copy.[55]

Owner exclusive e-books contain the strictest type of security that Microsoft Reader introduces. The restrictions are very stringent since it uses classic DRM technologies[56]. The purchaser can not buy the e-book without opening the Microsoft Reader first. As soon as Microsoft Reader is opened the book downloaded gets attached to the PC's Microsoft Passport account[57]. Copying and circulation of the e-book is thus inhibited for the e-book can only be opened with the computer with which it was downloaded.[58]

Purchased copies of George Orwell's 1984 and Animal Farm has been erased by Amazon.com from purchaser's Amazon Kindles since the DRM arrangement spotted illegitimate use of the copies[59]. These actions taken have been critisized of being highly Orwellesque by commentators since Amazon.com has acted like the Big Brother from Orwell's 1984.[60][61][62][63]

---

[52]Coyle, K.,"The Technology of Rights: Digital Rights Management", (PDF). http://www.kcoyle.net/drm_basics.pdf, 19.11.2003, last checked on 26.10.2009

[53] ibid.

[54] ibid.

[55] Noring, J., "The Perils of DRM Overkill for Large Publishers", http://www.teleread.org/publishersdrm.htm, 2004, last checked on 26.10.2009.

[56] "Internet Music", http://www.bigurlpro.info/internet-music.html, last checked on 20.10.2009.

[57] ibid.

[58]Coyle, K.,"The Technology of Rights: Digital Rights Management", (PDF). http://www.kcoyle.net/drm_basics.pdf, 19.11.2003, last checked on 26.10.2009

[59] New York Times, "Amazon Erases Orwell Books From Kindle Devices", 07.18.2009, last checked on 26.10.2009.

[60]New York Times, "Amazon Erases Orwell Books From Kindle Devices", 07.18.2009, last checked on 26.10.2009.

Amazon CEO Jeff Bezos apologized from the consumers. The Free Software Foundation has invited Amazon to employ DRM- free e-book readers declaring that the erasel of the purchased copies by amazon.com is an example of the exorbitant power Amazon has to censor and control what people read though its software.[6465]

2.2.4. Watermarking

Watermarking is an identification technique, which can guarantee the integrity and authenticity of digital content[66]. It allows the protection system to be incorporated for the first time into the "fabric" of the content, rather than being added on as separate information[67]. When for example a DVD is copied, the watermark accompanies the copy, regardless of the copy being made legitimately or not[68]. Specialized comprehension and substantial computer power are needed to get rid of the watermark: it must be erased from each and every frame of the media content[69]. If the DVD player finds a watermark in the copy, it rejects to operate it and ejects it[70]. The DVD player will distinguish that the media content is on a recordable DVD

[61]Pogue, D., New York Times, "Some E-Books Are More Equal Than Others", http://pogue.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/, 17.07.2009, last checked on 26.10.2009.

[62]arstechnica.com, Why Amazon went Big Brother on some Kindle e-books", http://arstechnica.com/tech-policy/news/2009/07/amazon-sold-pirated-books-raided-some-kindles.ars., 17.07.2009, last checked on 26.10.2009.

[63]Cashmore, P.,"Big Brother: Amazon Remotely Deletes 1984 From Kindles". http://mashable.com/2009/07/17/amazon-kindle-1984/., 17.07.2009, last checked on 26.10.2009.

[64]Frauenfelder, M., "Amazon zaps purchased copies of Orwell's 1984 and Animal Farm from Kindles". http://boingboing.net/2009/07/17/amazon-zaps-purchase.html, 17.07.2009, last checked on 26.10.2009.

[65] "Internet Music", http://www.bigurlpro.info/internet-music.html, last checked on 20.10.2009.

[66] Commission of the European Communities, Commission Staff Working Paper on Digital Rights, Background, Systems, Assessment, Brussels, 14.02.2002, SEC (2002) 197, available at http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/doc/workshop2002/drm_workingdoc.pdf, at page: 19, last checked on 22.10.2009.

[67] ibid, p:19.

[68] ibid, p:19.

[69] ibid, p:19.

[70] ibid, p:19.

(which being illegitimate) because the watermark technology is boosted with a "wobble"[71]. The wobble is an exclusive number stamped into the fabric of the DVD disc. It is encrypted to tally the watermark[72]. The system actually introduces a "tattoo" into the film and a "tattoo" into the disc[73]. These "tattoos" need to correspond each other -if they do not, or if one of them is lacking, this shows that an illegitimate copy has been produced, which the player will reject to operate[74]. The watermark/wobble system can be modified to authorize one generation private copies but impede any copying from those copies[75].

2.3. Digital Rights Management and Privacy

In fundamental concepts, DRM (…) can affect privacy because its information amassment and wiretapping capabilities can bestow copyright industries with quite specific and formerly devoid information about the reading, listening and viewing fashions of consumers[76]. Each separate access that a consumer makes with regard to a work can be registered by a DRM system[77]. For example, copyright holders are capable of knowing how a consumer made the on-line payment for a movie, how many times that movie is watched, whether any parts of it is being copied or whether it

[71] ibid, p:19.

[72] ibid, p:19.

[73] ibid, p:19.

[74] ibid, p:19.

[75] Commission of the European Communities, Commission Staff Working Paper on Digital Rights, Background, Systems, Assessment, Brussels, 14.02.2002, SEC (2002) 197, available at http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/doc/workshop2002/drm_workingdoc.pdf, at page: 19, last checked on 22.10.2009

[76] Cameron A., Digital Rights Management: Where Copyright and Privacy Collide, Canadian Privacy Law Review, 2004

[77] Cameron A., Digital Rights Management: Where Copyright and Privacy Collide, Canadian Privacy Law Review, 2004

was sent to someone else[78]. The specific information collected by DRM can later be used to build up detailed profiles of consumers[79].

DRM can become an important risk for privacy since it flows information about each separate access or use of the content it protects[80]. Both the essence of this information and the degree of its detail are remarkable[81].

In addition to the essence and specification of the information gathered by DRM, one of the most agonizing facets of DRM's effect on privacy is the fact that DRM is gathering information while consumers are involved in activities in places when and where they would likely have no apprehension of being surveiled – DRM gathers information while consumers are reading, watching or listening to media , consistently in the privacy of their houses or other private places[82].

Like other kinds of wiretapping, the form of DRM-based surveillance and data gathering described above can invade privacy in and of itself[83]. However, because of the quality of the activities consumers are involved in while being surveiled by DRM; DRM might as well hinder privacy in the shape of decreasing the autonomy and intellectual freedom of consumers[84].

IT specialists have addressed on the privacy issues related to DRM technologies[85].According to a paper entitled, *Privacy Engineering for*

[78] ibid.

[79] ibid.

[80] ibid.

[81] ibid.

[82] ibid.

[83] ibid.

[84] ibid.

[85] Steve Kenny & Larry Korba, "Privacy Rights Management for Digital Rights Management" (2002). An abstract can be found at www.cbpweb.nl/documenten/art_Kenny_Privacy_rights_

management_2002.htm.

Digital Rights Management Systems[86], privacy concerns arise in a number of ways, including:

- ID linkage**:** This DRM type beseeches the consumer to hand over an ID number that attaches the consumer's personal information (name, address, transaction history, etc.) with the hardware or the software a person intends to use.[87] These hardwares or softwares link to a rights server and when a user attempts to use a hardware or software , or makes updates or changes in the hardware of software, the rights server registers these changes or updates using the before registered ID handed over by the consumer[88].

- User tracking via download or subscription service: This DRM type complements the above mentioned ID linkage model[89]. The DRM operation entails that the consumer reconfirm that he will not make a copy of the product for resale or distribution[90].

2.3.1. The Sony Rootkit Incident and Its Implications

2.3.1.1 The Sony BMG Rootkit Software

In 2005, Sony published CD's, which included two different digital rights management systems; namely XCP software and Mediamax software[91].

[86] Joan Feigenbaum, Michael J. Freedman, Tomas Sander and Adam Shostack, PrivacyEngineering for Digital Rights Management Systems at www.homeport.org/~adam/privacyeng-wspdrm01.pdf.

[87] Cavoikian A., Information and Privacy Commissioner/Ontario, Privacy and Digital Rights Management: An Oxymoron?, 2002.

[88] Cavoikian A., Information and Privacy Commissioner/Ontario, Privacy and Digital Rights Management: An Oxymoron?, 2002.

[89] Cavoikian A., Information and Privacy Commissioner/Ontario, Privacy and Digital Rights Management: An Oxymoron?, 2002.

[90] Cavoikian A., Information and Privacy Commissioner/Ontario, Privacy and Digital Rights Management: An Oxymoron?, 2002.

[91] Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007, p:172.

These DRMs aimed at restricting disc-to-disc copying and preventing the distribution of musical works and sound recordings on peer to peer networks. The TPMs were created to restrict how customers could use music included in Sony BMG CDs[92].

First, Sony BMG outsourced a United Kingdom company namely First 4 Internet to develop a Windows copy protection program called XCP (extended Copy Protection) software[93].

In September 2005, John Guarino, the heir of TecAngels, found out that some of his customers' PC's had been influenced by an incomprehensible rootkit software[94]. He had to reinstall the computer systems in order to get rid of the software. Guarino then found out that his own PC had been infected by a similar rootkit[95]. He concluded that the responsible was a Sony BMG album called *Touch,* by the R&B singer, Amerie. The CD had included form of DRM that has installed the rootkit[96]. He sent the logs to a computer security firm, F-Secure[97]. F-Secure were worried that the rootkit could hinder the security of PCs by rendering them open to viruses, Trojan horses and malicious software[98]. F-Secure informed Sony BMG of the issue on 4 October 2005.[99]. Sony BMG did not reply to the concerns in fatly[100].

On 31 October 2005, an Mark Russinovich, wrote his blog that he was surprised to find out that a rootkit software had been installed on his PC by

[92] ibid, p:172.

[93] ibid, p:173.

[94] ibid, p:173.

[95] ibid, p:173.

[96] ibid, p:174.

[97] ibid, p:174.

[98] Roush, W. (2006), 'Inside the Spyware Scandal', Technology Review, 109 (2), 48-57 at 49.

[99] Roush, W. (2006), 'Inside the Spyware Scandal', Technology Review, 109 (2), 48-57 at 50

[100] ibid.

a Sony BMG CD[101] The post in the blog created a public outcry, which reached the big media like USA Today and BBC[102]. Some computer security companies declared that the Sony BMG software was a "spyware" because the rootkit was installed on computers without the consumer's authorization[103]. The software hindered the privacy of users, and the security of their computers. Furthermore, the rootkit could not be removed without the help of Sony BMG[104].

2.3.1.2. Lawsuits

In November 2005, the EFF sent an open letter to Sony BMG, declaring considerations on the XCP and SunnComm MediaMax software.[105]The EFF asked Sony BMG to request the return of all CDs that included the XCP and SunnComm MediaMax software, give back the price of infected CDs, and compensate consumers for any damage to their computers incurred by the effected CDs, including the time, effort and money needed to compensate the damage[106]. The EFF has brought an action on behalf of consumers against Sony BMG before the Superior Court of the State of California[107]. Sony BMG agreed to close the case with a settlement in December 2005[108]. As part of the settlement with consumers, Sony BMG replaced CD with

[101] Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007, p:174

[102] Geist, M. (2005), 'Sony's Long-term Rootkit CD Woes', BBC News, 21 November; and Kantor, A. (2005), 'Sony: The Rootkit of All Evil?', USA Today, http://www.usatoday.com/tech/columnist/andrewkantor/2005-11-17-sony-rootkit_x.htm, 17 November.

[103] Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007, p:175

[104] ibid, p:175.

[105] ibid, p:175.

[106] ibid, p:175.

[107] Hull v. Sony BMG Music Entertainment, No. BC343385(Cal.Super.Ct.Nov.21, 2005), http://www.eff.org/IP/DRM/Sony-BMG/sony_complaint.pdf.

[108] Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007, p:177

another CD free of the rootkit[109]. Sony also granted consumers with the option of $US7.50 plus one free album download, or three free albums downloads[110]. Sony BMG made some commitments with regard to the future of TPMs. The company consented not to produce or circulate audio CDs with XCP Software, or MediaMax 3.0 or MediaMax 5.0. Sony BMG undertook that it would notify any security risk in copy-control software in a fast and transparent way in future[111].

According to Michael Geist The European Union Copyright Directive and the US DMCA have legal rules governing TPMs but the rootkit scandal showed that there is the need for more harmonized consumer legal protections from TPMs.[112] The disclosure requirements brought for Sony in the case settlement showed that TPMs are like cigarettes and alcohol and they should contain warnings on their negative consequences.[113]

[109] Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007, p:177.

[110] ibid, p:177.

[111] ibid, p:178.

[112] ibid, p:179.

[113] ibid, p:179.

CHAPTER 3

EUROPEAN DATA PROTECTION LAW

After having examined the global developments on DRMs in the previous chapter, this chapter focuses on EU Data protection law, Chapter 4 will be dealing with EU Intellectual Policy Law, aiming at showing the interaction of these two sets of legal rules and making the privacy complications of DRMs clear.

3.1. General Principles of Community Law

The EU considers privacy a fundamental human right[114]. As a result of the lobbying activities of the Article 29 Working Party the right to data protection has been inserted as a fundamental human right to the Charter of Fundamental Rights of the European Union.

The recognition of a constitutional right to data protection in the EU Charter has been welcomed by commentators for several reasons[115]. It was first welcomed for bringing together on one hand the achievement of free movement of personal information and on the other hand the protection of fundamental rights of individuals[116]. According to Poullet and Gurtwirth the recognition of a fundamental right to data protection in the Charter added emphasis to the overshadowed fundamental rights dimension of the Directive[117]. The authors observed that it allowed for a sensible

[114] Bergkamp, Lucas, EU Data Protection Policy, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Dirven Economy, Computer Law and Security Report Vol.18 no.1., 2002, p: 33.

[115] ibid.

[116] Poullet Y., Gutwirth S., The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?, Brussels, 2008, p:570-610

[117] ibid.

constitutional division of labor. It was also welcomed for solving legal problems unanswered by ECJ Case law. Since data protection unequivocally protected values that are not in the centre of privacy[118] such as fair processing, consent or legitimacy, questions regarding these problems could not satisfactorily be met by the case law of European Court of Human Rights[119]. Poullet and Gurtwirth commented that the clear inclusion of a right to have compliance with all data protection rules controlled by an independent establishment, as is laid down by the last paragraph of Article 8 of the Charter, granted the Data Protection Authorities and Article 29 Working Party an important l place that was lacking in ECHR Case Law and the Case Law of European Court of Human Rights[120]. That the Charter extended the protection of personal data to private relations and private sector has also been welcomed by the commentators[121].

ON 13 December 2007, the European Council held in Lisbon approved the Reform Treaty[122], which replaced the abandoned Constitutional Treaty[123]. Under the Treaty, the Charter of Fundamental Rights has become a binding instrument[124].

That data protection being regarded and treated as a fundamental human right under EU law has raised several criticisms. These criticisms together with overall review of EU's Data Protection policy will be included in the

[118] De Hert, P.& Gutwırth, S., 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E.Claes, A Duff & Gutwırth (eds..), Privacy and the criminal law, Antwerp/Oxford, Intersentia, 2006, 61-104.

[119] Poullet Y., Gutwirth S., The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?, Brussels, 2008, p:570-610.

[120] Poullet Y., Gutwirth S., The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of 'reflexive governance'?, Brussels, 2008, p:570-610

[121] ibid.

[122] An incomplete version of Treaty of Lisbon was published in the OJ [2007] OJ C 306/1.

[123] Kacrorowska Alina, European Union Law, Routledge.Cavendish, Taylor and Francis Group, London and New York, 2009 p:43.

[124] ibid, p:43.

last part of this Chapter after providing an explanation on the basic data protection concepts introduced by EU Data Protection Legislation.

3.2. General Data Protection Directive

3.2.1. Background of the General Data Protection Directive

In the context of a single European market, it is vital that there should be no barriers to the movement of information between Member States. The principle of freedom of movement of goods and services has been quite succeeded and in this age of technology, a single European market would be implausible if the same freedom of movement has not been succeeded concerning personal data[125].

Conventional rules for data protection among Member States are endowed by the General Data Protection Directive. The statutory protections laid down by national data protection legislation diversified before the entry of the Directive[126]. The hypothesis behind the Directive was that; if all the Member States ratified acceptable standards for protection of personal data, the free movement of personal data within the Community would be succeeded.

The Directive was shaped in early 1990s and officially ratified in 1995[127]. The adoption of the Directive took almost five years due to difference of understanding between Member States and holders of different rights. The first proposal was published in 1990[128] which provided different systems for public and private sector. The differentiation of public and private sectors

[125] Bainbridge, David, Introduction to Informaion Technology Law, Six Edition, Pearson Longman, 2007 p: 499

[126] Solove, Rotenberg, Schwartz, Information Privacy Law, Apsen Publishers, New York, 2006 p:900

[127] ibid, p:900.

[128] COM (90) 314 final-SYN 287, OJ C 277, 05.11.1990, p:3.

was the position of some Member States such as Netherlands.[129] The divergence between public and private sector receded in another proposal published in 1992.[130] However this proposal was found by data users as being very restrictive and highly difficult to comply with. The Commission responding to some of the concerns of data users, made changes to reduce the financial burden of data users for the sake of retaining the principle of protecting the individuals' right to data protection[131].In December 1999, the Commission sued five Member States (France, Ireland, Germany, Luxembourg and the Netherlands) before the European Court of Justice for falling short of implementing the Directive. By the time of writing this thesis the five countries mentioned have all implemented the Directive[132].

The purpose of the Directive was simplifying the free flow of personal data within the EU by building up coordinately high data protection standards in all EU members.[133] The General Data Protection Directive can be considered as a general framework legislative instrument which has, as its principle aims:

- The protection of individuals privacy in relation to the processing of personal data; and

- The harmonization of data protection laws of the Member States[134].

3.2.2. Data Protection Principles Laid Down by the Directive

The Directive inflicts obligations on the processors of personal data. It entails technical security and the notification of individuals whose data are

[129] Bainbridge, David, Introduction to Informaion Technology Law, Six Edition, Pearson Longman, 2007 p: 499.

[130] COM (92) 24 final-SYN 393, OJ C 311,27.11.1992, p:38.

[131] Bainbridge, David, Introduction to Informaion Technology Law, Six Edition, Pearson Longman, 2007 p: 500

[132] ibid, p:500.

[133]Solove , Rotenberg, Schwartz, Information Privacy Law, Apsen Publishers, New York, 2006 p:900

[134] Carey, Peter, Data Protection, A Practical Guide to UK and EU Law, Oxford University Pres, 2004 p: 6.

being gathered, and sketches out conditions under which data transfer may take place. The directive also grants people important rights to control the use of their data[135]. Regulatory authority of data, enforcement rules, and measures are also key features of the directive[136].

Data protection principles laid down by the General Directive can be summarized as follows[137].

- **Legitimacy**: personal data can be processed only for particular purposes[138].

- **Consent**: personal data can be collected and processed only upon the open consent of the data subject to their processing. According to the Directive processing of personal data by private sector companies or profit-seeking public companies can be permitted only if the data subject gives his/her open consent.[139].

- **Finality**: personal data can only be collected for clear, open, and legitimate purposes and may not be processed more in a way adverse to those purposes[140].

- **Sensitivity:** the processing of personal data, which are specifically sensitive for the data subject, shall be subject to more rigid rules in comparison with other personal data[141].

---

[135] Solove, Rotenberg, Schwartz, Information Privacy Law, Apsen Publishers, New York, 2006, p: 900.

[136] ibid, p: 900.

[137] Kuner, Christopher, European Data Privacy Law and Online Business, Oxford University Press, 2003, p:17.

[138] ibid, p:17

[139] Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008, p:8.

[140] Kuner, Christopher, European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, Second Edition, 2007, p: 17.

[141] Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008, p:8.

- **Transparency**: the data subject must be given information pertaining to data processing relating to him[142].

- **Data Subject Control**: the data subject shall be able to circumvent and prompt the processing of his personal data[143].

- **Data Minimization:** processing of personal data must be restricted to the minimum essential quantity[144].

- **Minimal Disclosure:** the making public of personal data shall be restricted and can only happen when certain conditions are met[145].

- **Proportionality**: personal data must be sufficient, consistent and proportionate with regard to the purposes for which they are gathered and processed[146].

- **Purpose Specification**: personal data can only be gathered for legitimate, particular, lawful reasons and can not be processed in ways that are not accordable with the reasons for which they have been gathered[147].

---

[142] Kuner, Christopher, European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, Second Edition, 2007, p: 17.

[143] Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008, p:8.

[144] Kuner, Christopher, European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, Second Edition, 2007, p: 17.

[145] Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008, p:8.

[146] Kuner, Christopher, European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, Second Edition, 2007, p: 17.

[147] Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008, p:8

- **Confidentiality and security**: personal data should be processed after technical and organizational actions to provide confidentiality and security are taken.[148]

- **DPA Control**: DPAs should be supervising the processing of personal data[149].

- **Information Quality:** Personal data must be collected and processed accurately, and they should be relevant with respect to the purposes for which they are collected and processed[150].

3.2.3. Types and Categories of Data

- **Personal Data**

  Personal data is any data that can be used to identify an individual[151]. In this context "Personal data" is any information which relates to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, especially with reference to particular information about him. Such information may include an identification number or other information characteristic to his identity.

  According to the Article 29 Working Party, a natural person is "identified" if, within a group of individuals, he or she is differentiated from all other members of the group. The individual is

[148] Kuner, Christopher, European Data Protection Law, Corporate Compliance and Regulation, Oxford University Press, Second Edition, 2007, p: 17.

[149] ibid, p:17.

[150] Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008, p:8.

[151] ibid, p:8.

"identifiable" when, he can be identified but not been identified yet. [152].

- **Sensitive Data**

The Data Protection Directive established a type of data called 'sensitive data.[153]' Under the Directive, further legal protections are provided to sensitive data which are thought to be able to breach fundamental rights or privacy by their nature[154]. A data controller that processes sensitive data can only do it when he satisfies certain conditions laid down by the Directive[155]. These measures include conditions for data controllers to get open rather than closed consent, apply the security measures and restrict the forms of processing that may be performed[156].

- **Anonymous and Pseudonymous Data**

"Anonymous data" in the context of the Directive can be described as any information that relates to an unidentifiable natural person. Here the natural person can not be identified either by the data controller or by any other person even if they consider all the tools which might help to identify that person. "Anonymised data" is the previously anonymous data that was related to an identifiable person, but it is not possible to carry out the identification any more.

[152] Article 29 Data Protection Working Party, 01248/07/EN, WP 136, Opinion 4/2007 on the concept of Personal Data, 20. June 2007, p: 12.

[153] Carey, Peter, Data Protection, A Practical Guide to UK and EU Law, Oxford University Pres, 2004 p: 21.

[154] Reed, Chris and Angel John, Computer Law, The Law and Regulation of Information Technology, Sixth Eddition, Oxford University Press 2007, p: 476.

[155] Carey, Peter, Data Protection, A Practical Guide to UK and EU Law, Oxford University Pres, 2004 p: 21.

[156] Reed, Chris and Angel, John, Computer Law, The Law and Regulation of Information Technology, Sixth Eddition, Oxford University Press 2007, p: 476.

[157]Pseudonymous data are data that can be linked to a natural person and they are also subject to protection law. [158]

- **Identification Data**

Personal data that permit the unequivocal identification of the data subject is called identification data.[159]

3.2.4. Data Protection Actors:

- **Data Subject**

Data subject is the individual protected by data protection legislation.[160] European data protection legislation applies to "personal data". Personal data is defined as any information which relates to an identified of identifiable natural person. Thus data subject is defined indirectly being persons protected by data protection law[161].

- **Data Controller**

Data Controller under the Directive is any natural or legal person that determines the aims and tools of the processing of personal data.

- **Data Processor**

[157] Article 29 Data Protection Working Party, 01248/07/EN, WP 136, Opinion 4/2007 on the concept of Personal Data, 20. June 2007, p: 21.

[158] Kuner, Christopher, European Data Privacy Law and Online Business, Oxford University Press, 2003, p:73

[159] Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008, p:9.

[160] Bainbridge, David, Introduction to Informaion Technology Law, Six Edition, Pearson Longman, 2007 p: 521.

[161] Kuner, Christopher, European Data Privacy Law and Online Business, Oxford University Press, 2003, p:54

Data Processor is a natural or legal person that processes personal data on behalf of the controller[162].

3.3. Directive on Privacy and Electronic Communications

The Directive on Privacy and Electronic Communications[163] entails data protection in electronic communications sector. Telecommunications, faxes, e-mail, the Internet are considered as electronic communications.[164]

Following are the main characteristics of the Directive on Privacy and Electronic Communications:

- **Scope**

  Despite service providers working over the public Internet are most particularly covered, the Directive entails all public electronic communication systems. [165][166].

- **Security and Confidentiality**

  Under the Directive providers of publicly available electronic communications services must take necessary cautions to protect the security of their services. Member States are also expected to ratify national legislation to provide the confidentiality of communications.[167]

---

[162] Artcile 2 of General Data Protection Directive.

[163] Dir (EC) 97/66 of the European Parliament and the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector, [1998] OJ L 24/1.

[164] Kuner, Christopher, European Data Privacy Law and Online Business, Oxford University Press, 2003, p:20.

[165] Boone, Kevin, EU Directive on Privacy and Electronic Communications,

[166] Recital 10 reads that: In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals. Directive 95/46/EC applies to non-public communications services.

[167] Art. 4 (1).

- **Restrictions on Data Processing**

  Traffic data relating to users processed and retended by an electronic communications service provider must be deleted or anonymized when it is no longer necessary for the purpose of the services provided[168].

- **Unsolicited communications**

  The service providers have to get the prior consent of the subscriber before using automated calling systems for direct marketing.[169]

- **Use of Cookies and Spyware**

  Under the Directive cookies and other invisible surveillance systems that can collect information of end users, such as 'spyware' may only be involved if the user has been given clear information about the aim of any such invisible operation. The users should be granted the rights to reject involvement of such systems that will help the user to find out what kind of access to his computer are agreeable and which are not[170].

- **Location data**

  GSM operators have to get the clear approval of the user before circulating or processing location data.[171]

[168] Article 6 (1).

[169] Millar, Sheila A., EU Adopts Directive on Privacy and Electronic Communications.

[170] New Privacy Rules for Digital Networks-Directive kicks in today, IP/03/1492, 31.10.2003.

[171] Ibid.

3.4. Criticism of EU's Data Protection Policy

The necessity of the EU's data protection legislation has been questioned in the literature.[172] It is argued that the way EU balanced different interests concerning information society does not match economic facts[173]. Information being at the very center of market economy is dependent to the availability of data. Information has two facades[174]. First being the increased productivity and the efficiency of production thanks to the free flow of information[175] and second being the readiness of consumers to give up privacy for economic interests in their data. [176] It is argued that privacy options forced by governments, limited consumer freedom in two ways. First, consumer freedom is limited by such forced options by not letting consumers to trade based on their own privacy choices[177]. Second, consumer freedom is limited indirectly by putting the introduction and marketing burdens of new products and services on the shoulders of consumers[178]. It is further argued that the advantages and disadvantages of data protection are not shared equally by rich and poor[179] since the poor had less options but paid higher prices when compared to the rich. It is also argued that the EU data protection regime restricted competition. Elimination of privacy protection as an element of competition between suppliers in a market caused direct restrictions. [180] EU did not allow divergence s on "privacy product's by providing a "high level of protection" and thus described the "privacy product" that companies must offer. As a

[172] Bergkamp, Lucas, EU Data Protection Policy, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Dirven Economy, Computer Law and Security Report Vol.18 no.1.

[173] ibid, p: 35.

[174] ibid, p: 35.

[175] ibid, p: 35.

[176] ibid, p: 35.

[177] ibid, p: 37.

[178] ibid, p: 37.

[179] ibid, p: 38.

[180] Bergkamp, Lucas, EU Data Protection Policy, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Dirven Economy, Computer Law and Security Report Vol.18 no.1., 2002, p: 39.

consequence, any competition related to privacy protection is eliminated since all companies had to provide the same level of protection[181].

According to Bergkamp, privacy law indirectly impeded competition in different markets by impeding the accessibility of consumer data in the market. Thus data protection system has put new participants and minor companies in a competitive disadvantage[182]. Litan argued that opt-in regime created barriers to entry by minor and often more creative firms and organizations[183].

Commentators also argued EU data protection system also negatively disturbed international trade by setting new barriers to entry. Non EU traders are put in a more difficult position in getting into the EU Market because consumer data is not available to them and it makes targeted marketing more difficult for them[184].

[181] ibid, p: 39.

[182] ibid, p: 39.

[183] Litan RE., Balancing Costs and Benefits of New Privacy Mandates, AEI-Brookings Joint Center for Regulatory Studies, Working Paper 99-3, April 1999.

[184] Bergkamp, Lucas, EU Data Protection Policy, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Dirven Economy, Computer Law and Security Report Vol.18 no.1., 2002, p: 39

CHAPTER 4

EUROPEAN INTELLECTUAL PROPERTY LAW

4.1. Introduction

Apart from permitting people to possess automobiles, PCs, houses , or other tangible goods, intellectual property law permits people to own rights to control works of art and computer software etc.[185]. This second type of ownership as a rule is called intangible or intellectual property[186].

'Intellectual Property' is the name conferred to legal rights that protect works of art, inventions and commercial goodwill[187]. Fundamentally, intellectual property rights are shaped to accommodate reliefs against those who take away the products of another person's ideas or work without permission[188]. Intellectual Property is usually designated as non-tangible property that the product of intellective processes and whose worth is based upon some idea. [189].

In general terms, the concept 'intellectual property' can be considered as covering anything originating from the functioning of the human brain: designs, abstractions, images, stories, songs- the list is continuous[190]. It is an

[185] Adam D. Moore, Intellectual Property and Information Control, 2001, Transaction Publishers, New Jersey, p: 9.

[186] ibid, p: 9.

[187] Bainbridge, David, Introduction to Information Technology Law, Six Edition, Pearson Longman, 2007 p: 9.

[188] ibid, p: 9.

[189] Adam D. Moore, Intellectual Property and Information Control, 2001, Transaction Publishers, New Jersey, p: 13.

[190] J Lloyd, Ian, Information Technology Law, Oxford University Press, 2004, p:364.

extensive concept used to blanket a group of legal rights protecting non-physical property which are often of big economic importance[191]

Intellectual property rights, basically the copyright system, are related to the protection of rights in some aesthetic or creative work[192]. Protection of works of literature, art, music is in the center of the copyright system. Copyright is the right to establish who can copy a creative work[193]. That is to say copyright protects works from being copied without permission[194]. Copyright exceeds the limit of just copying, however, expands to other acts like adapting the work, performing the work in public, communicating the work to third parties[195]. Copyright protects the consolidated exposition of the work: the exclusive way in which the thoughts are articulated is copyrighted, not the thoughts themselves[196].

Together with copyright, artistic works are sometimes protected by neighboring rights: dances by dancers, sound recording, and broadcasts are examples[197].

When the nature of software is considered, it will be clear that it stands at the apertures of the industrial and intellectual property systems. Software, in particular at the stage of operating systems, is related to functioning. At the beginning, it may be claimed that the aim of intellectual property rights is to

[191] P Terence, European Intellectual Property Law, Ashgate Dartmouth, 2000, p: 3.

[192] J Lloyd, Ian, Information Technology Law, Oxford University Press, 2004, p:364.

[193] R Marlin-Bennett, Knowledge Power, Intellectual Property, Information and Privacy, Lynne Rienner Publishers, Inc., 2004, p: 35.

[194] Bainbridge, David, Introduction to Informaion Technology Law, Six Edition, Pearson Longman, 2007 p: 9.

[195] ibid, p: 9

[196] R Marlin-Bennett, Knowledge Power, Intellectual Property, Information and Privacy, Lynne Rienner Publishers, Inc., 2004, p: 35

[197] ibid, p: 36

give rights on the individual responsible for realizing ideas and discounting these to a useable format[198].

4.2. The EU's Intellectual Property Policy

Times are changing and needs of the post-industrial information society are different from those of the industrial society. Information has become a commodity as valuable as coal or steel in this new era[199]. The services sector now provides most of EU's income. Since they affect media and knowledge and other industries, the copyright industries are crucially important to the European Community. According to the European Commission, copyright industry proffered more than €1,200 billion to the economy of the European Union, created value added of €450 billion, and employed 5.2 million individuals in 2000. The total gross value added, that benchmarks wealth added to the economy, illustrated more than 5.3 % of the total value added for the 15 EU Member States. With regard to employment, the industries added 3.1 % of total EU employment[200]. Software and electronic information services have become important growing components of the sector[201].

4.2.1. Competence of European Community in Harmonization of Intellectual Property

The capability of the European Community to harmonize national laws in the area of Intellectual Property emanates from Article 295 and particularly from Article 95 of the Treaty establishing the European Community (EC

[198] J Lloyd, Ian, Information Technology Law, Oxford University Press, 2004, p:365

[199] ibid, p:363.

[200]European Commission, The EU Single Market, Copyright and Neighbouring Rights, http://ec.europa.eu/internal_market/copyright/index_en.htm, last checked on 25.10.2009.

[201] J Lloyd, Ian, Information Technology Law, Oxford University Press, 2004, p:363.

Treaty)[202]. These articles designate the Community to enact laws in the area of intellectual property and the realization of an internal market without boundaries[203].

The European Commission in addition to the European Council and the European Parliament is the organ responsible of formulating harmonization laws in the area of IP and of surmounting international trade agreements, encompassing those related to IP issues[204].

The Commission has communicated an action plan in the field of intellectual property including the following components:

- Harmonization of national laws to protect intellectual property rights;
- Advanced law application training programs;
- Education programs to boost understanding among consumers of the adverse effects of buying pirated products;
- The filing of a study for determining a system for gathering, evaluating and comparing data related to counterfeiting and piracy[205].

The European Commission has 36 departments, conferred to as 'Directorates-General' (DGs) and 'services' (such as the Legal Service)[206] DG Trade, DG Taxation and Customs Union, DG Internal Market, DG Enterprise of the European Commission are involved in the enforcement of

[202] Maximilliano Santo Cruz S., Intellectual Property Provisions in European Union Trade Agreements, Implications for Developing Countries, ICTSD Intellectual Property and Sustainable Development Series, June 2007, p:4.

[203] ibid, p:4.

[204] ibid, p:4.

[205] Vrins, O. and Schneider M., Enforcement of Intellectual Property Rights Through Border Measures, Oxford University Pres, 2006, p: 29.

[206] ibid, p: 30.

intellectual property [207]. The technical collaboration in the areas of legislative consultation, awareness boosting in the profit sector and civil society, fall within the scope of responsibilities of the DGs of the European Commission. [208].

Among others separation and surveillance of internal and external intellectual property policies in compliance with trade policies of the European Union are within the ambit of the undertakings of DG Trade[209]. To provide greater awareness and enforcement in the field intellectual property rights is an important policy of the Union[210]. Contribution to the application of adequate standards for intellectual property around the world , collaboration with developing and under developed countries, joining in the combat against breaches; providing that such rights are ancillary to public health concerns , innovation and technology assignment are in the ambit of DG Trade's policy in the area of intellectual property. [211]

The responsibility of DG Customs Union and DG Taxation is to protect and preserve the Customs Union and to make sure the standard implementation of the origin rules[212]. Customs offices are charged with new assignments pertaining to the preservation of both the customary trader and the consumer together with their orthodox role of collecting duties.[213] There are many improvements that led the customs offices to endorse new strategies to

[207] ibid, p: 30.

[208] ibid, p: 30.

[209] ibid, p: 30.

[210] ibid, p: 30.

[211] ibid, p: 30.

[212] Vrins, O. and Schneider M., Enforcement of Intellectual Property Rights Through Border Measures, Oxford University Pres, 2006, p: 32.

[213] ibid, p: 32.

combat with counterfeiting and piracy like EU enlargement, the expansion in fraud and organized crime[214].

The Internal Market DG deals with the 'knowledge based' features of the Single Market[215]. Harmonization of the legislation of Member States as to industrial property rights to circumvent barriers to trade is a part of its responsibility.[216] In order to eliminate barriers to trade and to adopt the scheme to new kinds of abuse, there has been substantial intellectual property harmonization in the EU[217]. The responsibility of Internal Market DG's is to implement this *'acquis'* and to renew and enact it to new improvements in the related markets and technology[218].

The IPR Helpdesk (www.IPR-Helpdesk.org) is created by DG enterprise with the aim of helping future and current contractors participating in European Community financed R&D projects on intellectual property rights issues[219]. The IPR Helpdesk also provides counseling to the Community in international research projects.[220] The Helpdesk has a more comprehensive purpose to create awareness of European research community on IPR matters with a stress to their European ambit[221]. It also carries out seminars and education courses on intellectual property issues[222].

The two main constitutional treaties of the EU, namely the Treaty on European Union (Maastricht Treaty) and the Treaty of Rome were modified

[214] ibid, p: 32.

[215] ibid, p: 33.

[216] ibid, p: 33.

[217] ibid, p: 33.

[218] ibid, p: 33.

[219]ibid, p: 33.

[220]ibid, p: 33.

[221] Vrins, O. and Schneider M., Enforcement of Intellectual Property Rights Through Border Measures, Oxford University Pres, 2006, p: 34.

[222] ibid, p: 34.

by the Treaty of Nice. Treaty of Nice addressed to achieve an array of institutional concerns to get ready for the EC enlargement through future candidate countries[223]. The Treaty of Nice also involved in some Intellectual Property issues. The Commission was given capability to negotiate and finalize agreements regarding the commercial facets of IP. The Commission also was granted capability to negotiate agreements in non-commercial facets of IP where "the Council, acting unanimously on a proposal from the Commission and after consulting the European Parliament" so agreed[224]. Secondly the Council, after being advised by other EU Institutions, was entitled to organize chambers or judicial panels to settle at first instance different types of action or proceedings put forward in the area of intellectual property[225]. Intellectual Property actions have been divided between different chambers of the Court of First Instance[226].

4.2.2. Internal Priorities in Intellectual Property

In 2000 European Heads of State enacted the Lisbon Agenda[227]. The Agenda has put the strategic objective of making EU the most competent and active knowledge-based market in the world by 2010. The answer to the accomplishment of this agenda was determined as being innovation. [228]

Among others, the expansion and extension of the internal market were determined as the main fields pertaining to the application of the Lisbon Agenda by the European Commission. This involved the establishment of a

[223] Maximilliano Santo Cruz S., Intellectual Property Provisions in European Union Trade Agreements, Implications for Developing Countries, ICTSD Intellectual Property and Sustainable Development Series, June 2007, p:4.

[224] ibid, p:4.

[225] ibid, p:4.

[226] ibid, p:4.

[227] ibid, p:4.

[228] ibid, p:4.

Community Patent System, the fostering of an "Internal Market in knowledge" and the expedition of the demand part for "content"[229].

The EU through the promulgation of green and white papers determines its exclusive priorities and policies involving those on intellectual property.[230] Green papers deal with certain policy areas, they are discussion papers communicated by the Commission. Related parties, establishments and individuals are called for to join in a procedure of advising and debate through these papers. In some situations they augment to consecutive legislation[231]. White papers are documents that promulgate proposals for Community action in a certain field. White papers in some situations are issued after a green paper to start a consultation process at European level. White papers contain official proposals in specific policy fields and are used as tolls to development while green papers bring about a scale of ideas submitted for public debate.[232] These papers can directly involve intellectual property issues [233] or be indirectly related to them.

Secondary legislation accommodates a broad scale of regulation on Intellectual Property[234] that can be in the shape of Directives, Regulations, Recommendations or Decisions.[235]

[229] ibid, p:4.

[230] ibid, p:5.

[231]Europa, Gateway to the European Union, http://europa.eu/index_en.htm, last checked on 25.10.2009.

[232] ibid.

[233] E.g. Green Paper on Combating Counterfeiting and Piracy in the Single Market.

[234] ibid, p:5.

[235]Treaty Establishing the European Community-Article 249: "In order to carry out their task and in accordance with the provisions of this Treaty, the European Parliament acting jointly with the Council, the Council and the Commission shall make regulations and issue directives, take decisions, make recommendations or deliver opinions. A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States. A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods. A decision shall be binding in its entirety upon those to whom it is addressed. Recommendations and opinions shall have no binding force.

EU Enforcement Directive (2004/48) was legislated in 2004[236] with the purpose of providing "a high, equivalent and homogenous level of protection in the internal market"[237]. It was aimed to remove discrepancies between the regimes of the Member States.

4.2.2.1.Harmonization

International agreements, the community level rules and national laws are three different sets of rules that built the foundation of European intellectual property law.[238] Intellectual property rights intrinsically carry the following complications for the European Market when conceded from a legal point of view:

1. Possible conflict with competition rules due because of the exclusivity of intellectual property rights. (Art. 85-86 EC)
2. Conflict with the free movement of goods within the internal market because of the territoriality of national intellectual property rights (Article 30 EC).[239]

The principle of exclusivity of Intellectual Property Rights provides the possessor of intellectual property rights to inhibit specific acts of third parties such as dispersing the protected good. This inevitably eliminates third parties free market entry and also influences the competitive configuration of the market[240]. However the principle of exclusivity

[236] Maximilliano Santo Cruz S., Intellectual Property Provisions in European Union Trade Agreements, Implications for Developing Countries, ICTSD Intellectual Property and Sustainable Development Series, June 2007, p:5.

[237] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

[238] Thumm N., Intellectual Property Rights, National Systems and Harmonisation in Europe, Physica- Verlag Heidelberg, 2000, Germany, p:66.

[239] ibid, p:66.

[240] ibid, p:66.

attempts to reimburse for the public good nature of technological knowledge[241]. EU Law does not openly harmonize the relationship between intellectual property rights and competition rules (Articles 85-86 EC) however European Court of Justice case by case deals with the principles pertaining to this relationship. [242]

4.3. Review of EU's IP Legislation

4.3.1. Enforcement Directive

On 15 October 1998, the European Commission started a public discussion on *Combating Counterfeiting and Piracy in the Single Market*[243] with a green paper in order to debate on the subject with related parties[244]. Administrative collaboration between the national organs, action by the profit sector, the adequateness of technical protection measures, sanctions and other tools of providing sound application of intellectual property rights were the issues contained by the Green Paper. [245] A follow-up to the Green Paper was communicated by the Commission on 30 November 2000. [246] The Commission in the above mentioned follow up declared that it would be issuing Directive proposal aiming at the harmonization of the provisions of the Member States for the purpose of succeeding equivalent protection in the internal market[247]. The Commission issued its proposal on

[241] ibid, p:66.

[242] Thumm N., Intellectual Property Rights, National Systems and Harmonisation in Europe, Physica- Verlag Heidelberg, 2000, Germany, p:66

[243] Combating Counterfeiting and Piracy in the Single Market-Green Paper, COM (98) 569 Final, Brussels, 15.10.1998.

[244] Vrins, O. and Schneider M., Enforcement of Intellectual Property Rights Through Border Measures, Oxford University Pres, 2006, p: 22.

[245] ibid, p: 22.

[246] Communication from the Commission the the Council, the European Parlimaent and the Economic and Social Committee, Follow- up to the Green Paper on combating counterfeiting piracy in the Single Market,COM (2000) 789 Final, Brussels, 30.11.2000.

[247] ibid, p: 22.

20 March 2003[248].On 29 October 2003, the Economic and Social Committee gave its Opinion[249250]. On 27 November 2003, the Committee on Legal Affairs and the Internal Market of the European Parliament voted some changes to the Commission proposal[251]. It also stated to the Council of Ministers its expectation that the Directive be legislated by the European Parliament and Council at first reading.[252] The proposal has been revised many times by the Intellectual Property Working Party of the Council. The Directive on Intellectual Property Enforcement was legislated by the European Parliament on 9 March 2004. [253] The Council of Ministers approved it in April 2004. Member States had to apply the enforcement articles into their national law within two years[254].

4.3.2. Directive 2001/29/EC

The Directive[255] deals with the legal protection of copyright and neighboring rights in the scheme of the common market, with special focus on the information Society[256]

Under the Directive Member States are to grant certain exclusive rights to copyright holders. The Directive lays down some exceptions and restrictions to the exclusive reproduction right. In some cases Member States may grant

[248] ibid, p: 22.

[249] Opinion of the European Economic and Social Committee on the 'Proposal for a Directive of the European Parliament and the European Council on the measures and procedures to ensure the enforcement of intellectual property rights. (OJ C32 of 5.2.2004,15).

[250] Vrins, O. and Schneider M., Enforcement of Intellectual Property Rights Through Border Measures, Oxford University Pres, 2006, p: 22.

[251] ibid, p: 22.

[252] ibid, p: 22.

[253] ibid, p: 22.

[254] Vrins, O. and Schneider M., Enforcement of Intellectual Property Rights Through Border Measures, Oxford University Pres, 2006, p: 22

[255]Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19.

[256] Art.1 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001.

exemptions and limitations with the condition that copyright holders get enough reimbursement. The Directive also grants the choice to the Member States to legislate exemptions and limitations when specific conditions for each exemption are satisfied.

Member States have to ensure sufficient legal protection against the abuse of any efficient technological measures. The Directive also lays down some constraints pertaining to rights-management information. The Member States must ensure legal protection against deliberate removal or modification of rights-management information. Member States must also set suitable penalties and compensations regarding the breach of rights and obligations laid down by the Directive and must provide that those penalties and reimbursements are enforced. The measures applied by the member states must be efficient, equitable and persuasive[257].

The Directive also requires that Member States provide right holders whose rights breached with the right to bring an action for damages and for the abduction of breaching material together with devices or components.

On 30.11.2007 the first report[258] on the implementation of the Directive on the harmonization of certain aspects of copyright and related rights in the information society (2001/29/EC) was issued.

The report reviewed the implementation of the Directive with regard to the development of the digital market.[259]

The report discovered that in order to immune specific cases from copyright protection local courts have usually used a teleological explanation of the

[257] Art.9

[258] Commıssıon Staff Workıng Document, Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Brussels, 31.11.2007, SEC(2007) 1556.

[259] Commıssıon Staff Workıng Document, Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Brussels, 31.11.2007, SEC(2007) 1556, p:3

reproduction right. For example, in the *Copiepresse* case[260], a Belgian court ruled that the copy of a web-page reserved in the memory of Google's systems and the exposure of a link making the cached copy available to the public breached both the reproduction right and the right of making available to the public[261]. However the court did not rule that Google displace the cache copies from its search engine. It only ruled that the links to the cache copies be displaced from the Google search website. The court declared that the reproduction of news in its cache copies were an essential part of the technical mechanism of filing webpages[262].

Google has created a service called "Google.news" in 2002 which is a search engine based on the filing of press articles published on the internet. This service was working in Belgium with the name "Google.Actualités".[263]

Copiepresse argued that the service "Google.Actualités" was farther than a search engine since it worked as a "portal to the written press". According to Copiepresse, Google was reproducing and displaying an important part of the body of the articles without getting the consents of the sites of the newspaper publishers on behalf of whom it advocates the interests[264]. On 9 February 2006, Copiepresse submitted a pleading for appropriation to the court of first instance in Brussels.[265]

During the trial Google claimed that the Google.News service was grounded by article 10 of the European Convention of Human Rights which secures

[260] Google v Copiepresse, Brussels Court of First Instance (TGI), 13th February 2007.

[261] Commıssıon Staff Workıng Document, Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Brussels, 31.11.2007, SEC(2007) 1556, p:4

[262] ibid, p:4.

[263] English Translation of the Ruling of Google v Copiepresse, Brussels Court of First Instance , 13th February 2007, available at, http://www.copiepresse.be/13-02-07-jugement-en.pdf.

[264] ibid.

[265] ibid.

freedom of expression. [266] Google persisted that the limitation of the right of the freedom of expression argued is neither relevant nor balanced as Google News is a free instrument for reception of information which does nothing other than providing an suggestive starting point in the search for information on the Internet.[267]

The Court declared that the freedom of expression that adequately granted the freedom to accept and disclose information was not unconditional and it might be subject to protocols, conditions, limitations or sanctions as are foreseen by law. [268] The Court reflected that some exceptions to the copyright from objecting the reproduction or communication of their work to the public were grounded on the freedom of expression, for example, citations[269].

However Copiepresse claimed that it was not possible in this situation to refer to the exercise of a right of expression when Google is concerned since the system applied by GoogleNews was not a natural human and Google did not engage any head editor for choosing the articles. [270]

The Court went on examining if there was breach of copyright and if Google might present an exception.[271]

The Court found out that Google reserved a copy of the news pages in its memory, this copy was linked to HTML code of the related pages or it was switched into computer language. [272] The Court envisaged that there was

[266] ibid.

[267] ibid.

[268] ibid.

[269] ibid.

[270] ibid.

[271] ibid.

[272] English Translation of the Ruling of Google v Copiepresse, Brussels Court of First Instance , 13th February 2007, available at, http://www.copiepresse.be/13-02-07-jugement-en.pdf.

reproduction in the digital platform from the time that there was a saving or reservation of signals in any kind of memory and Google therefore was the creator of the reproduction.[273]

Copiepresse and the volunteer third party arbitrators deemed the service "Google.Actualités" or "Google.News" to suggest more than a lucid search engine service and should be certified as an "information portal". They pinpointed that "Google.Actualités" offered content to Internet users without a prior search.[274]

Copiepresse accused Google of getting the text precisely from their sites, by copying the headlines of commentaries and the slogans, without having taken their previous permission and they argued that this was a breach of copyright[275].

Google disputed that while reproducing and making protected works public they directed the Internet user along a hyperlink, to the site of source with an approach to consult the article and thus Google restricted itself with making that article more available.[276]

Google also debated that the components contained on the home page of its website "Google.Actualités" like the headlines of the commentaries and the first sentence the said commentary were original components advantaging from the protection of copyright law. Google acknowledged that it was able to preserve the exceptions designated by law on copyright, like the exceptions of citing and reporting news[277].

[273] ibid.

[274] ibid.

[275] ibid.

[276] ibid.

[277] ibid.

Following conclusions were reached by the Court:

- that Google can not claim any exception as designated in copyright law,
- that the actions of Google News and the employment of the Google "cache" violated copyright law[278];

The Court instructed Google to discard from all these sites, particularly from Google News, all commentaries, images and graphic designs of authors for whom the complainants proved that they represent the rights[279].

Private copying is not regarded as a right under the Directive. Accordingly, in the Belgian *Test Achats* case[280], the court ordered that the private copying exception does not establish an applicable right[281].

A Belgian consumer organization, Test-Achats, initiated a suit against four major music companies alleging that their use of technological protection measures on numerous CDs prompted copyright violation.[282]

Test-Achats argued that the DRM system impeded consumers from creating their own private copies of the copyrighted works and it moreover impeded them from listening to CDs on different mechanisms with audio devices such as PCs and DVD players[283]. Test-Achats also claimed that the music companies are violating the right of the user to create private copies

[278] English Translation of the Ruling of Google v Copiepresse, Brussels Court of First Instance , 13th February 2007, available at, http://www.copiepresse.be/13-02-07-jugement-en.pdf.

[279] ibid.

[280] Test Achats v EMI Recorded Music Belgium et al., Brussels Court of Appeal, 9 September 2005, case 2004/AR/1649.

[281] Commıssıon Staff Workıng Document, Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Brussels, 31.11.2007, SEC(2007) 1556, p:5

[282] de Keersmaeker, Christine , "Belgium: Technological Protection Measures on CD's", 08.04.2005, available at http://www.mondaq.com/article.asp?articleid=31935.

[283] ibid.

and requested a general measure to stop the usage of DRM[284]. Test-Achats also grounded their argument on the presence of a tax on digital reproduction hardware[285].

The defendants claimed that "private copying" is just an exception to copyright protection and an exception cannot be interpreted in a way so as to create a right to private copying. It can just be deemed as a defense in case of a law suit brought by the copyright owners[286]. In other words, the exception does not grant the user a right to ask from copyright holders that they provide hat private copies can always technically be performed[287].

The accomplishment of Test-Achats in its argument was debatable from the commencement since the EU Directive on Copyright and the Information Society permitted the employment of technical protection measures.[288].

Brussels Court of First Instance decided in favor of the defendants on May 25th, 2004[289]. The Court affirmed that private copying is just an exception to the copyright[290]. According to the ruling the exception just meant that it was not essential for a user to get the approval of the right holder to create a private copy[291]. The legal outcome of making a private copy is that it can not be considered as a violation of copyright[292] but this does not grant the consumer the right to demand from the copyright holders that a private copy always technically can be created[293].

[284] ibid.

[285] ibid.

[286] ibid.

[287] ibid.

[288] ibid.

[289] ibid.

[290] ibid.

[291] ibid.

[292] ibid.

[293] ibid.

In the *Mulholland Drive* case[294] which was initiated by a consumer organization, the French discussed the same problem. The court ruled that the private copy exception should be negated if it is at odds with the normal exercise of a work.

In 2003 a consumer together with the Association UFC-Que Choisir initiated a law suit against the producers of the movie Mulholland Drive[295]. The consumer claimed that the DVD he legally possessed was guarded by DRMs that did not allow the consumer to create a copy in order to watch it on a VHS system at his parents' house[296]. The DVD did not signify whether it would function specifically with some devices or not[297]. The Court of Appeal in Paris ruled on 4 April 2007 that the private copying of a specific work can not be considered as a right but it is rather a legal exception to the principle of copying the total text without the permission of the copyright holder[298]. In other words private copying can not be regarded as a right but it is rather an exception and it is not possible to initiate a legal suit grounding the claims to an exception.[299] It was also stipulated by the Court that if different legal conditions are satisfied such an exception can serve as a defense in a law suit of counterfeit.[300]

Member States are permitted to accommodate an exception to the reproduction right for specific reproductions performed by certain

[294] Studio Canal et al. v S. Perquin and Union federale des consommateurs Que choisir, Cour de Cassation, 1st civil section, 28 February 2006, case N° 549, Bull. 2006 I N° 126 p. 115 ("Mulholland Drive"), overruling Studio Canal et al. v S. Perquin and Union federale des consommateurs Quechoisir, Paris Court of Appeal, 22 April 2005, available at http://www.juriscom.net/documents/caparis20050422.pdf. The Court of Appeal found that the application of a copy control mechanism on the DVD limited consumers' rights by preventing them from making a private copy.

[295] EDRI-gram , "Private copy explained by Court of Appeal in Paris", 12.04.2007, available at, http://www.edri.org/edrigram/number5.7/private-copy-france, last checked at 20.01.2010.

[296] ibid.

[297] ibid.

[298] ibid.

[299] ibid.

[300] ibid.

organizations[301]such as libraries under Article 5(2) (c) of the Directive. According to the report, national arrangements especially those concerning the number of copies permitted for protection or format-shifting purposes differentiated but Member States have made arrangements which fall within the scope of Article 5(2) (c).

The description of efficient technological measures under Article 6(3) includes a wide scale of technologies. In this context, a technological measure is deemed to be efficient if it succeeds in the protection purpose[302]. According to the report, most Member States have taken the decryption of technological protection rights directly. Slovakia and Sweden have not harmonized this requirement at all[303]. The Helsinki District Court, in criminal case put forward by the providers of evasion software allocated on the Internet, decided that the CSS mechanism employed on DVDs was inefficient since it did not succeed in the protection purpose. The said TPM was broken in 1999 by a Norwegian hacker and the tools to break the TPM have become easily accessible on the Internet[304].

The Finnish Copyright Council communicated a consultation on 29 August 2007. According to the consultation a TPM can no deemed to be inefficient based on the possibility of a “crack" since those “cracks” should happen often in reality[305].

Under Article 8(3) of the Directive Member States are impelled to accommodate right holders with the right to search for a sanction against

[301] Commıssıon Staff Workıng Document, Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Brussels, 31.11.2007, SEC(2007) 1556, p:5.

[302] Commıssıon Staff Workıng Document, Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Brussels, 31.11.2007, SEC(2007) 1556, p:8

[303] ibid, p:8.

[304] ibid, p:8.

[305] ibid, p:8.

agents whose supplies are employed by a third party to breach copyright or related rights[306]. In a small number of Member States[307], Article 8(3) has been transposed to national legislation[308]. According to the findings of the report Article 8(3) fell within the framework of current legislation of different Member States. For the implementation of Article 8(3), the violation of copyright by a third party is enough. [309]

The Commission promulgated a Green Paper on copyright in the knowledge economy. The Green Paper aligns with the function of copyright in promoting circulation of knowledge for research, science and education. The Green Paper aimed at starting a discussion on the long-run future of copyright policy in these areas. Copyright policy has to a greater extent appeared as a crisscross issue, since it deals both with the internal market and information society.

4.4. IP Data Protection Interaction

4.4.1. The Impact of EU Data Protection Law on DRMS

As indicated in the third chapter of this research the General Data Protection Directive is the most significant privacy tool for the European Union as a whole. The DPD produces guidance on data protection across a large scale of sectors[310].

In order to protect the privacy and interests concerned, data protection systems pinpoint the regulation of diverse stages in the processing of

[306] ibid, p:9.

[307] Austria, Greece, Latvia, Belgium.

[308] ibid, p:10.

[309] ibid, p:10.

[310] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 424.

personal data[311]. A DRMS may be influenced by the laws to the extent it processes such data[312].

The term "personal data" is often described with a general and flexible attitude. The decryption of the Directive pinpoints the possibility of data to enable separating a certain person from a group of persons.

It is the in the capacity of the data protection actors to monitor the rules of data protection laws since they master the tools and objectives of the processing of data on other individuals[313]. These actors are called "controllers". The DPD[314] describes a "controller" as the person that on his own or together with others decides on the objectives and tools of the processing of personal data"[315].

"A controller" and a "processor" are not the same actors. [316] A processor is a person that processes personal data representing the data controller[317]. It is the obligation of the controllers to provide that processors perform their duties according to the laws that are ratified in compliance with the Directive[318].

[311] ibid, p. 426.

[312] İbid, p. 426.

[313] ibid, p. 427.

[314] See: Article 2(d) of the DPD

[315] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 427.

[316] See: Article Art. 2(e) of the DPD.

[317] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 428.

[318] See: Art. 17(2)–(3); see also Art. 16 of DPD

4.4.1.1. Core Data Protection Principles

The implementation of data protection rules to a DRMS indicates that the system operators should process personal data complying with the fair and lawful processing principle[319]. Lawful processing, in summary means that personal data must be gathered by fair and lawful tools , it should be restricted to what is essential to succeed the objective for which the data are gathered ,[320]making public of personal data to third parties must happen only with the permission of the data subject[321],personal data must be sufficient , integrated and consistent with the reasons for which they are processed[322], security measures should be applied to preserve personal data from accidental or illegitimate revelation, demolition or change[323], data subjects should be able to join in, and apply a degree of control over, the processing of data on them by data controllers[324], parties in charge of processing data on other persons must be liable for abiding by these principles[325].

Apart from the above mentioned rules; persons should be given the chance to stay anonymous[326327], they should be noticed about data on them carried by others[328], and entirely mechanical assessments of an individual's

[319] See: especially DPD, Art. 6(1)(a).

[320] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 429.

[321] ibid, p. 429.

[322] ibid, p. 429.

[323] ibid, p. 429.

[324] ibid, p. 429.

[325] ibid, p. 429.

[326] See especially DPD, Art. 6(1)(e) and (c), together with Arts. 7–8.

[327] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 429.

[328] DPD, Arts. 10–12.

personality should not be used to make conclusions about that person's interests"[329]

4.4.1.2. Basic Conditions for Data Processing

Under the Directive, the collection and further processing of personal data is inhibited if the processing does not meet one or more of the following conditions[330].

(a) Clear permission of the data subject to the processing should be received[331];
(b) The processing should be essential for the performance of a contract with the data subject[332];
(c) The processing should be essential in order to satisfy the requirements of a legal obligation by the controller[333];
(d) The processing should be essential for the preservation of crucial interests of the data subject[334];
(e) The processing should be essential for performing an obligation in the public interest.
(f) The processing should be essential"[335] for the satisfaction of legitimate interests that prevail over the conflicting interests of the data subject. [336]

[329] ibid, p. 429.

[330] ibid, p. 430.

[331] See Art. 7(a) of DPD.

[332] See Art. 7(b) of DPD.

[333] See Art. 7(c) of DPD.

[334] See Art. 7(d) of DPD.

[335] See Art. 7(f) of DPD.

[336] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 430.

The conditions mentioned in paras. (a)[337], (b)[338], (c)[339] and (f)[340] are most related with the functioning DRMS[341]. The condition in para (a) requires that the data subject makes clear his permission to personal data relating to him being processed."[342] Permission doesn't have to be writing but to comply with this rule; the accurate registration of permission on paper or electronic device can be helpful[343]. It can also be argued that the permission given by data subjects should leave no suspicion that he/she has given permission.[344]

In the framework of a DRMS, just the conclusion by a consumer of a transaction with a system operator can be considered as permission to the operator's storage of some data on the consumer[345]. But, this permission will only be deemed to be given for the storage steps, which the consumer could possibly foresee or about which the consumer is given previous information[346]. Under the Directive notification to the consumer will have to be performed in such a manner that it provides data processing being fair when the interests of data subjects are concerned[347]. Thus, it can be claimed that notification must take place before the purchase contract or transaction

[337] The data subject's "unambiguous" consent to the processing.

[338] The condition that the processing should be "necessary" for the "performance" or conclusion of a contract with the data subject.

[339] The condition that the processing should be "necessary" for compliance with a "legal obligation" on the data controller.

[340] The condition that the processing should be "necessary" for the pursuance of "legitimate interests" that override the conflicting interests of the data subject.

[341] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 430.

[342] ibid, p. 430.

[343] ibid, p: 430.

[344] ibid, p:430.

[345] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 430.

[346] ibid, p. 430.

[347] ibid, p. 430.

is concluded and it should compromise active participation of operator to the process.[348]

However unless the person is provided with a chance to give permission to registration, the registration of that person's access to the server of a DRMS is not legitimate under para. (a) Since there is the possibility that the person in question was not going to browse different pages of the server[349]. Furthermore, based on the hypothesis that cookies build up personal data, a server functioning with a system that fabricates and sets cookies at the first access to the server as a matter of course, will fall outside the scope of para. (a)[350]. Actually, in the framework of DRMS operations, such a cookies system may scarcely satisfy any conditions in Art. 7 other than those set forth in paras. (b)[351] and (f)[352][353].

The condition laid down in Art. 7(b)[354] can be satisfied in the framework of a DRMS and pertaining to the processing of data of the purchaser if a contract has been concluded by the purchaser and a system operator[355]. The condition can also be satisfied concerning the processing of data relating to a browser if the processing is performed at the request of the data subject

[348] ibid, p. 430.

[349] ibid, p. 431.

[350] ibid, p. 431.

[351] The condition that the processing should be "necessary" for the "performance" or conclusion of a contract with the data subject.

[352] The condition that the processing should be "necessary" for the pursuance of "legitimate interests" that override the conflicting interests of the data subject.

[353] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 431.

[354] The condition that the processing should be "necessary" for the "performance" or conclusion of a contract with the data subject.

[355] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 431.

before concluding a contract."[356][357] In both situations it is critical to determine which data processing can be considered as necessary.[358]

The necessity principle includes two conditions:

- that the processing is about an important social or commercial need; and
- That the processing is balanced when the purpose of the contract is considered[359].

Stringency of these conditions will depend on the type of data processing carried out.[360]. The conditions will be clearly satisfied if the system operator in charge records only the data that are necessary for the performance of the provisions of a contract concluded by the service provider and consumer[361]. The consumer's name and address, the information about the product and its cost and the date of the sales will most possibly be among the data recorded.

To what degree para. (b)[362] Can be applied to legitimize the surveillance of consumers' transactions with the purpose to control accordance to the contract after the contract is entered into by the parties is more ambiguous. [363]Such surveillance may be related with the performance of a contract but this does justify such surveillance totally since the surveillance has to be

[356] See Art. 7(b) of the DPD.

[357] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 431.

[358] ibid, p. 431.

[359] Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems, Imprımatur, Institute for Information Law, June 1998, at page 18.

[360] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 431.

[361] ibid, p. 431.

[362] The condition that the processing should be "necessary" for the "performance" or conclusion of a contract with the data subject.

[363] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 431.

balanced in order to satisfy the "necessity" requirement[364]. The surveillance may be related to a broad scale of personal data that are not necessary in terms of compliance[365].

The requirement set forth by Art. 7(c)[366] can have significance where data controller has legal duties in front of other DRMS actors[367]. However, the term "legal duty" needs to be interpreted in a fashion that it does not contain only duties under a contract.[368] If the term is not interpreted in this fashion under para. (c)[369] data controllers would be able to process personal data just by creating a contract to which the data subject need not necessarily be a party[370].

The broadest of requirements in Art. 7 is the requirement laid down in para. (f)[371372]. The Directive does not give sufficient data on how divergent interests referred to in para. (f) are to be proportioned[373]. However under the Recital, Member States are to safeguard "effective competition" when divergent interest are concerned[374].

---

[364] ibid, p. 431.

[365] ibid,, p. 431.

[366] The condition that the processing should be "necessary" for compliance with a "legal obligation" on the data controller.

[367] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 431.

[368] ibid,, p. 432.

[369] The condition that the processing should be "necessary" for compliance with a "legal obligation" on the data controller.

[370] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 432.

[371] The condition that the processing should be "necessary" for the pursuance of "legitimate interests" that override the conflicting interests of the data subject.

[372] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 432.

[373] ibid, p. 432.

[374] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 432.

To what degree para. (f)[375] legitimizes the employment of cookies upon a persons connection to a DRMS system, where the permission of the person is not received, is regarded as an interesting problem. [376] The problem is only significant if the data recorded can be deemed "personal" according to Art. 2(a) of the Directive[377][378]. Recital 25 in the DPEC[379] preamble indicates that cookies may be a "legitimate and useful tool" for making "provision of information society services" easier[380]. How cookies can be deemed in favor of information society depends on the definition of benefits and the kind of data recorded[381]. If succeeding in providing best conditions for marketing is determined as the benefit then the use of cookies might be justified. However even if cookies are justified in this way, their employment will still conflict with the data subjects' benefits in the protection of their privacy.[382]

[375] The Condition that the processing should be "necessary" for the pursuance of "legitimate interests" that override the conflicting interests of the data subject.

[376] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 432.

[377] Article 2 (a) of the DPD reads as follows: 'Personal data 'shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

[378] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 432.

[379] Recital 25 of the preamble of the DPEC reads as follows: Such devices, for instance so called "cookies", can be legitimate and useful tool, for example, in alaysing the effectiveness of website design and advertising, and in veryfying the identity of users engaged in on-line transactions. Where such devices, for instance cookies are intended for a legitimate purpose, such as to facilitate the provision of of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordaance with Directive 95/46/EC about the purposes of cookies or terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or smilar device stored on their terminal equipment. This is particulary important where users other than the original user have access to the terminal equipment ant hereby to any data containing privacy-sensitive information stored on such equipment. Information and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or fequesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.

[380] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 433.

[381] ibid, p. 433.

[382] ibid, p. 433.

Under the DPEC[383][384] employment of cookies is allowed only for justified reasons with the requirements that data subjects be informed of their employment , and granted the option to reject , their employment. [385] For the employment of cookies literal permission of data subjects is not deemed as a necessary requirement[386][387]. The Directive doesn't indicate when data subjects should be informed of cookie employment[388]. From the stand point of privacy advocacy a data subject should be informed before a cookie is installed on his computer[389].

4.4.1.3. Sensitive Data

The requirements for data processing become stricter when sensitive data is involved[390]. A DRMS might process sensitive data because the system operator is enabled to record certain personal choices of consumers.[391] For instance , where a consumer concludes a contract to purchase a product which contains a specific religious or sexual element, and the product is recorded matching the consumer's name or any other specific identifier, thus sensitive data about the consumer gets processed[392]. Such a data

[383] Art. 5(3) of the DPEC reads as follows: Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

[384] See also above footnote 725 for the Recital 25 of the preamble of the DPEC.

[385] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 433.

[386] See above footnote 725 for the Recital 25 of the preamble of the DPEC.

[387] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 433.

[388] ibid, p. 433.

[389] ibid, p. 433.

[390] See Art. 8 of DPD.

[391] ibid, p. 435.

[392] ibid, p. 435.

processing is troublesome since the link between the product's sensitive element and the consumer's personality in this occasion becomes remote. However, just the purchase of a product by a person should not necessarily indicate that the product represents the consumer's personal taste; there is the chance that he may be performing a scientific or educational study over that product[393]. How troublesome such a processing may turn into depends on various components like the qualities of the product. For example a scholarly exercise on sadomasochism will be inclined to disclose less about the consumer's personal sexual choices than a video–clip illustrating sadomasochistic ceremonies. The character of the activity is also important. For example a single activity will disclose less about the consumer's personal choices than a series of activities that join in a similar motif[394].

4.4.1.4 Purpose Specification

Another principle that influences DRMS is the purpose specification principle which is frequently called the finality principle as well[395]. The most explicit interpretation of the principle in the Directive is under Art. 6(1) (b)[396] which provides that personal data should be collected for designated, clear and justified purposes and should not any more is processed in a fashion inconsistent with those purposes[397]". In the framework of DRMS, this condition is critical when purchaser–/browser–related data are involved[398].

---

[393] ibid, p. 435.

[394] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 435.

[395] ibid, p. 436.

[396] Art. 6(1)(b) reads that Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

[397] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 436.

[398] ibid, p. 436.

The principle in Art. 6(1) (b)[399] aims at both ensuring that data are processed in ways that conform to data subjects' reasonable expectations[400] and ensuring that data are used for purposes to which they are suited. [401] Under Art. 6(1)(b)[402] , the purposes of recording by a DRMS operator of data of a consumer on a browser must be defined, documented and notified prior to such recording[403]. [404][405]. Furthermore the purposes of recording should be "legitimate"[406].

4.4.2. The Copyright Directive

The affect of DRMS on data protection is not only covered by data protection laws; but also intellectual property rules play an important part[407]. Arts. 6–7 of the Copyright Directive[408] are the most significant provisions of EU law in terms of DRMS[409]. These rules provide backing for DRMS

[399] Art. 6(1)(b) reads that Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

[400] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 436.

[401] ibid, p. 436.

[402] Art. 6(1)(b) reads that Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards.

[403] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 436.

[404] See also DPD Arts. 10 and 11.

[405] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 437.

[406] ibid, p. 437.

[407] ibid, p. 438.

[408] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19.

[409] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 438.

technologies.[410] According to Article 6, efficient "technological measures" must be furnished with sufficient legal protection against intentional violations[411] "Electronic rights management information" is dealt with by Article 7 (a) according to which illegitimate change or deletion is prohibited[412]. Article 7 (b) prohibits the circulation of copyrighted works after they are being changed where such circulation violates copyright.[413]

4.4.2.1. The Meaning of TPM

Whether the technological tools that surveil *usage* of copyright works can be deemed as "technological measures" according to CD Art. 6 is a significant problem.[414] If such tools are not deemed as "technological measures" their unemployment will not breach Art. 6(1)[415]. If such tools are deemed as "technological measures" their unemployment will be a violation of Art. 6(1)[416].

The Directive does not give an explicit answer to the question[417]. However, when a more flexible definition of "technological measures" is applied it is possible to decide that some surveillance tools may be covered by this flexible definition[418][419][420].

---

[410] ibid, p. 438.

[411] ibid, p. 439.

[412] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 439.

[413] ibid, p. 439.

[414] ibid, p. 439.

[415] Art. 6 (1) of CD reads that Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

[416] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 439.

[417] ibid, p. 440.

[418] "Any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder of any copyright [or related rights] [. . .]"

A technological measure should be involved in prevention of illegitimate actions in the due course of operation. This may indicate that surveillance tools which are not directly involved in such prevention are not deemed to be technological measures[421].

4.4.2.2. The Scope of RMI

"Rights management information" (RMI) dealt with Article 7 of the Copyright Directive is another significant data protection related issue.[422] To put it more clearly whether personal data is an essential element of RMI[423] or not is the issue. The answer to this question has significance because if such data are deemed to be essential elements of RMI, their modification or deletion by a consumer can be covered by Art. 7(1)[424][425]. According to the definition of Art. 7(2)[426] , "*information about the terms*

[419] Art. 6(3) of CD reads that for the purposes of the Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.

[420] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 440.

[421] ibid, p. 440.

[422] ibid, p. 443.

[423] ibid, p. 443.

[424] Art. 7(1) of CD reads as follows: Member States shall provide for adequate legal protection against any person knowingly performing without authority any of the following acts: (a) the removal or alteration of any electronic rights-management information; (b) the distribution, importation for distribution, broadcasting, communication or making available to the public of works or other subject-matter protected under this Directive or under Chapter III of Directive 96/9/EC from which electronic rights-management information has been removed or altered without authority, if such person knows, or has reasonable grounds to know, that by so doing he is inducing, enabling, facilitating or concealing an infringement of any copyright or any rights related to copyright as provided by law, or of the sui generis right provided for in Chapter III of Directive.

[425] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 443.

[426] Art. 7(2) of the CD reads as follows: For the purposes of this Directive, the expression "rights-management information" means any information provided by rightholders which identifies the work or other subject-matter referred to in this Directive or covered by the sui generis right provided for in Chapter III of Directive 96/9/EC, the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.

and conditions of use of the work or other subject matter" is considered as RMI[427]. Is the data on the identity of consumers covered in the "terms and conditions of use"?[428] Is personal data concerning the usage of the works covered by it? [429] The expression "terms and conditions of use" does not in the fist reading; contain such data since it involves data which is literally used.[430][431] However when the reality that how user specific some license terms are, it can be claimed that at least the identity of users are covered.

Another significant question concerning Art. 7(1) is whether the provision applies to the modification or deletion of RMI when such data is not incorporated to the copyright work[432]. For example according to Australian and Hong Kong copyright laws, RMI is only protected when it is incorporated to the copyright work. Similarly, components of RMI are not protected if they are once detached from the work involved. The transfer of the RMI back to a DRMS is piece of a continuous surveillance process[433] does not affect the non protection in front of law. Because according to the definition of RMI under Australian and Hong Kong legislation the information should be "attached" to a copy of a work[434]. However, the framework of RMI is not accordingly limited in when Art. 7(2)[435] of the Directive are concerned. By contrast, even when not incorporated a work, RMI is still covered by Art. 7[436] The deletion or modification of data about users will violate Art. 7(1) when the deletion or modification is carried out

[427] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 443.

[428] ibid, p. 443.

[429] ibid, p. 443.

[430] ibid, p. 443.

[431] ibid, p. 443.

[432] ibid, p. 443.

[433] ibid, p. 444.

[434] ibid, p. 444.

[435] ibid, p. 444.

[436] ibid, p. 444.

illegitimately and such data are to be deemed as an essential element of RMI.[437] Here, the reply to the question of "who is the related authority?" will be provided by data protection laws[438]. The question of "to what degree modification or deletion of the data is allowed by data protection legislation?"[439] is a more complex one. Because the answer changes according to the result of a sophisticated process of proportioning interests that necessitates the determination of what information processing can be deemed "necessary" in the present case[440]. According to the DPD processing of data on consumers doesn't necessitate the permission of the data subject where the processing is required by a contract or for a legal defense in a criminal proceeding[441]. If these conditions are construed broadly it can be claimed that consumers can not legitimately erase or change data about them recorded by DRMS operators[442].

4.5. The High Level Working Group on DRMs

On 14 February 2002, European Commission promulgated a Commission Staff Working Paper on Digital Rights, Background, System and Assessment[443]. Basic policies concerning the applicability of DRMs were covered in the Working Paper.

The Working Paper highlighted that the Commission's policy in the field of DRMs was governed by the Copyright Directive. It was also underlined that

[437] ibid, p. 444.

[438] ibid, p. 444.

[439] ibid, p. 444.

[440] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 444.

[441] ibid, p. 444.

[442] ibid, p. 444.

[443] Commission of the European Communities, Commission Staff Working Paper on Digital Rights, Background, Systems, Assessment, Brussels, 14.02.2002, SEC (2002) 197, available at http://ec.europa.eu/information_society/eeurope/2005/all_about/digital_rights_man/doc/workshop2002/drm_workingdoc.pdf, last checked on 22.10.2009.

the Commission among other entities had also been allocating funds for research in the area of DRMs since 1992.

It was observed by the Working Paper that the technological developments always had impacts on the legal system for copyright and has been at the center of the possibility for amendment[444]. Traditional copyright systems had supported offline services which created lower quality reproductions at high circulation costs.[445]. The Working Paper also observed that the digital world has changed the offline market and has created a very big market for content[446].

The European Commission established a High Level Group (HLG) on Digital Rights Management (DRM) issues in March 2004[447]. The Group was established with the involvement [448] of representatives of the content suppliers, writers and rights holders associations, software developers, hardware manufacturers, academicians, consumers and other related parties.[449] On 31st of March the HLG consorted to determine the problems convening DRM, to amalgamate the opinions of the different parties involved in DRM related problems and determine possible solutions.

- Interoperability provisions, embracing standardization improvements for DRM to satisfy users' anticipations,
- Acknowledgement and confidence by users with special stress on security and privacy,

[444] ibid, p:7.

[445] ibid, p:7.

[446] ibid, p:7.

[447] COM (2004) 61 of 03.02.2004 "Connecting Europe at high speed: recent developments in the sector of electronic communications"

[448] Members of the HLG DRM included: GESAC, IFPI, Vivendi, Eurocinema, FEP – Federation European Publishers, BBC, France Telecom, Vodafone, Fast Web, Philips, Nokia, Alcatel, Hewlet Packard, Siemens, New Media Council and BEUC. IFPI, Philips and HP have been the rapporteurs of the Group.

[449] High Level Group on Digital Rights Management, Final Report, March-July 2004, p:2

- Shift to lawful services,
- The significance of DRM when current rights management manners, notably the implementation of taxes,
- Evaluation of the implementations of DRM in the European markets (success stories, restrictions, and presumptions)[450].

The final report submitted on 8 July contemplated an agreement on main principles and consultations for impending actions. It included three main facets:

- DRM and Interoperability
- Private copying taxes and DRM
- Shift to lawful services[451].

According to the report, both the international and EU copyright scheme contribute to the legislative ground on which DRMS function. Especially, the WIPO Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty implore the legal perseverance of efficient technological protection measures[452] and rights management information.

The report has observed that the EU has performed its international undertakings according to both of these Treaties with the ratification of the Copyright Directive and especially Articles 6 and 7 of the Directive. EU data protection policy also builds up the guidelines according to which DRMs function[453].

[450] ibid, p:2

[451] ibid, p:2

[452] WCT (Article 11 and 12) and WPPT (Article 18 and 19) WIPO

[453] High Level Group on Digital Rights Management, Final Report, March-July 2004, p:2

The High Level Group observed that for the development of a lawful market on the internet reinforcing the shift of consumers from illegitimate file-sharing services to legitimate online services was crucial. According to the HLG, the amplifying return of lawful services in Europe was a proof that consumer appeal for legitimate service on the internet is getting more powerful. The accessibility of content from circulation channels and from the apparatus used was greeted by the HLG since it was considered as a recent and supplementary line for content owners and an appealing new occupation of mobile network services providers who are used to correlate big numbers of customers. Particular stress was made to being differential of privacy and data protection when online services are concerned.

The HLG on one hand stressing the importance of data protection related problems, on the other hand observed that the progress of the online market was hindered by the procreation of illegal services and large amount of digital piracy. According to HLG, online piracy had two prominent shapes: circulation of files by illegitimate internet sites; and peer-to-peer influx on file-sharing sites. HLG observed that these sites allowed users to circulate and shuffle digital files without being permitted to do so or without paying their prices. HLG also observed that these services did not contribute in creating any product but they earn millions of Euros from added spyware to the content that belong copyright holders. The report also highlighted that illegitimate file-sharing has led to investment deficit in content development, recession in the legitimate market, unemployment and relinquished taxes for governments.

4.6. Opinion of Article 29 Working Party

On 18 January 2005, Article 29 Working Party has promulgated a working document on data protection issues related to intellectual property rights.

The Working Party noted that the growing circulation of information due to the development of the Internet adjoined more and more with the problem of mastery over copyrighted works[454]. According to the WP the problems required solutions with regard to the rights and undertakings of actors benefiting from copyrighted works and their involvement in the management of digital rights[455].

The Working Party accepted the significance of applying sanctions to preserve the lawful interests of copyright holders against trickery[456].

The first facet the Working Party made reference was concerned with the digital management of rights since DRMs enabled the identification and mapping of consumers attaining copyright protected data on the Internet[457]. The second facet concerning the options handy for copyright holders is to coerce their rights against consumers who are doubted of breaching copyright[458].

In relation to the development of digital rights management, the WP noted that recent technologies for identification or mapping of users were not only being built up at the stage of sharing information but also at platform stage[459]

Concerning the sharing or downloading of copyrighted works on the Internet, the WP observed that the attainment of such information required

[454] Article 29 Data Protection Working Party, xxxx/05/EN WP 104, Working document on data protection issues related to intellectual property rights, 18 January 2005,p:2

[455] ibid,p:2

[456] ibid,p:2

[457] ibid,p:2

[458] Article 29 Data Protection Working Party, xxxx/05/EN WP 104, Working document on data protection issues related to intellectual property rights, 18 January 2005,p:2

[459] ibid,p:3

more and more primary checking of the user's identity which caused further mapping of consumers using tags.[460]

According to the WP, the purpose of checking and mapping is to control "a priori" every user that legitimately downloads information on the Internet. Most of copyright owners also carry out "a posteriori" inquiries against users doubted of breaching copyright.[461]

The Working Party elicited the core data protection principles and the ambit to which they will be implemented in the framework of digital right management and copyright execution[462].

The Working Party observed that sketching users has become simpler because of the employment of unique identifiers that allowed the interconnection of data concerning a single individual. Father it was stated in the Working Document that employment of unique identifiers within the structure of digital rights management enabled the sketching of the user in relation to the quality and quantity of works he confers.

Regarding the information of the data subject the Working Party decided that biggest possible openness should be accommodated concerning the functioning of the digital rights management system. The Working party deciding this, encompassed article 10 of Directive 95/46, according to which no information shall be collected concerning data subjects without prior notification addressed to them as to components like the aim of the processing, the information on the data controller, the receivers of data, and the presence of a right of access.

[460] ibid,p:3

[461] ibid,p:3.

[462] Article 29 Data Protection Working Party, xxxx/05/EN WP 104, Working document on data protection issues related to intellectual property rights, 18 January 2005,p:4

The Working Party concerning the purpose limitation principle indicated in the Working Document that personal data gathered from the user at his will or the data gathered due to its essential nature for the undertaking of the service should only be used in accordance with the indicated purpose. Recording the name and address of the user while payment is made a with a credit card and further use of that information for marketing purposes, after having articulated with the taste of the user was given as an example for discord with the principle.

The Working Party draw attention to the commencement of procedures by copyright holders which aim at inquiring suspected copyright violations regarding the amount of investigation powers.

The Working Party underlined data protection principles, concerning the investigations by copyright holders as the following:

- Principle of compatibility: The Working Party observed that right holders constructed their research basically on the building up of bottom lines accessible on-line. Exposure of copyright protected woks in peer-to-peer networks, they could reach to data such as date and time of suspected violation, qualities of the protected work, and also erratic identifiers such as nick names of the responsible of the possible violation. The Working paper also indicated that on the ground of the compatibility principle and also in accordance with the confidentiality principle contained in Directives 2002/58 and 95/46, data reserved by ISPs for particular reasons containing basically the fulfillment of a telecommunication service cannot be assigned to third parties except under determined conditions laid down by law.[463].

[463] Article 29 Data Protection Working Party, xxxx/05/EN WP 104, Working document on data protection issues related to intellectual property rights, 18 January 2005,p:7

- Role of Internet Service providers: The Working Party reminded that no organized responsibility of monitoring and cooperation could be dictated to ISPs, according to article 15 of Electronic Commerce Directive[464]. The Working Party emphasized that internet service providers could not be obliged to enable an "a priori" reserve of all traffic data concerning copyright except in particular situations where there is a sanction by law enforcement authorities. The Working Party has indicated regarding numerous events [465] that for the retention of traffic in particular occasions, there must be a justifiable need and the period of retention must kept as short as possible the retention must be clearly permitted by law.[466]

- Processing of judicial data: The Working Paper indicated that processing of data concerning criminal verdicts or security measures can be carried out only under firm conditions as laid down by article 8 of the Data Protection Directive. The working document marked the right of individuals to process judicial data in the course of their own legal actions but the same is not allowed to third parties under EU Data Protection Law.

The Working Party to conclude stated concerns about the lawful use of technologies to preserve works, also being harmful to the protection of personal data. As for the implementation of data protection principles with regard to the digital enforcement of rights, it has observed, a growing deficit between the protection of individuals in the analogue and digital worlds, particularly with regard to the quite normalized mapping and monitoring of individuals[467]. The Working Party called for creation of technical devices

[464] ibid, p:7.

[465] See for example Opinion 5/2002 adopted on 11 October 2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, 11818/02/EN/Final, WP 64.

[466] Article 29 Data Protection Working Party, xxxx/05/EN WP 104, Working document on data protection issues related to intellectual property rights, 18 January 2005,p:7.

[467] ibid,p:8

which are more transparent and employ less unique identifiers and give a choice option to the user.[468]

4.7. Remarks on the Interaction

The development of digital management rights systems has brought two conflicting interests into discussion. Copyright holders legitimate interest of effective enforcement of their rights and end-users right for data protection and privacy, needed to be balanced under legal systems.

The balancing of these two conflicting interests had to be worked out both on a legal and commercial plane. On the legal plane, an assessment of what is necessary for the effective enforcement of copyright in the light of privacy and data protection rights has been the ground of balancing the conflicting rights.

The question of how EU balanced these two conflicting interests required a research on both EU Legislation on Data Protection and Intellectual Property and the interaction of these two sets of legal rules. The interaction of intellectual property and data protection involved two critical areas in the EU. The EU had to balance the interests of copyright industries which are critically important to the European Community since they involve media, cultural, and knowledge industries and the data protection interests of consumers which is a constitutional right under EU Legal Regime.

The EU especially through the studies of working groups established by the Commission and the opinions of Article 29 Working Party on Data Protection, has given clear answers to the question of to what extend digital copyright can be enforced and which rules data protection rules should be abode by copyright holders.

[468] ibid,p:7

The answers given by the EU institutions on the interaction of data protection and copyright are important not only for current digital rights management systems but also for new technologies that may be developed for copyright protection. Since the data protection framework in which copyrights can be legitimately enforced has been made clear by the EU while discussing the interaction of data protection and copyright in the context of digital management rights systems.

The following Chapter 5 aims at evaluating the DRMs issue from the point of view of a developing country and finding an answer to the question of whether the above mentioned answers given by EU are also applicable to Turkey or not.

CHAPTER 5

IMPLICATIONS ON TURKEY

5.1. Introduction

This Chapter examines the implications of DRMs employment and the importance of data protection rules from the perspective of a developing country.

It is possible to argue that DRMs systems that enforce their own copyright protection policies without the necessity of applying the jurisdiction of different countries was a good idea especially for countries like Turkey where the regulatory system or the enforcement of laws do not restrict piracy to the extend necessary. According to the 2009 Progress Report, Turkey has made little progress in the area of copyright and neighboring rights. Piracy of books and other media, such as CDs, DVDs and copyright infringements remained widespread. Turkey's enforcement capacity was not found satisfactory.

It can also be argued that the use of DRM systems in Turkey has been much easier since these systems did not face the privacy restrictions set forth by EU Data Protection Directive when the DRM protected products are sold in Turkey. The 2009 Progress Report stated that with regard to the right to protection of personal data, Turkey needed to align its legislation with the data protection acquis, in particular Directive 95/46/EC, and, in that context, to set up a fully independent data protection supervisory authority.

Turkey lacking both the tools to prevent piracy and protect privacy has been one of the best markets for the use of DRM systems.

The following chapter will be summarizing the current situation of Turkey in relation to data protection and copyright and evaluating the implications of DRMs on developing countries like Turkey. Finally, Chapter 6 will be concluding with proposals for action in the fields of data protection, copyright and DRMs in Turkey.

5.2. Turkey's Legislative Frameworks

5.2.1. Legislative Framework of Privacy in Turkey

Turkey signed the Convention for THA Protection of Individuals with Regard to Automatic Processing of Personal Data[469] in 1981 but has not adopted it yet. Turkey has signed and adopted THA European Convention for THA Protection of Human Rights and Fundamental Freedoms.

5.2.1.1. Constitutional Framework

Article 20 of THA Turkish Constitution involves with privacy of persons and reads that, "Everyone has THA right to claim respect for his private and family life. Privacy of individual and family life shall not be breached[470]."

Article 20 impedes THA search or abduction of any individual, his/her private documents, or his/her assets unless there is a decision by a judge or unless there is a decision of an entity authorized by law in occasions where delay is considered detrimental.

Article 22 protects the confidentiality of communications and provides that, "Communication shall not be restricted nor its confidentiality be violated,

[469] Convention No. 108.

[470] See, Article 20 of Turkish Constitution.

unless there is decision of a judge or unless there is a decision of an entity authorized by law in occasions where delay is considered detrimental."

5.2.1.2. Data Protection Framework

- **The Draft Data Protection Law**

The draft law has been prepared in 2003 has not yet been ratified.

The draft, among others, includes the following provisions:

- General conditions for data processing,[471]
- Data subjects rights for getting information on data about them,[472]
- Transfer of data to foreign countries,[473]
- Rules for data processing by natural persons, private and public legal entities,[474]
- Establishment and responsibilities of the supervisory authority[475];
- Search for legal relief under civil and criminal law.[476]

The following analysis will try to provide a criticism of Turkish Draft Law from a comparative law point of view taking Polish Data Protection Act into consideration.

Article 3 of the draft law, provides definitions. Some of these definitions are quite problematic due to different reasons. Personal data is defined in Article 3 as "Any information related to an identified or identifiable person" however, it is quite obvious that the definition and regulation of personal data deserves being provided a separate article in the law when its

[471] See, Article 4 of the Draf Law.

[472] See Article 7 of the Draft Law.

[473] See Article 10 of the Draft Law.

[474] See Articles 13-15 of the Draft Law.

[475] See Articles 20-36 of the Draft Law.

[476] See Section 7 of the Draft Law.

importance is considered. Personal data, in Polish Data Protection Act, is regulated under article 6 in detail and the way it is regulated is much more aligned with EU Data Protection Directive.

"The processing of personal data" which is one of the most important issues that should be dealt with is just mentioned in Article 3 among the definitions and then it is regulated under Article 4. The title of the article is quite misleading as it is "The quality of personal data". It can be concluded that the draft law is not in harmony with the Directive, because the detailed rules foreseen in the Directive for data processing are not adopted in any sense. However the Polish Data Protection Act regulates the principles of data processing in its Chapter three between articles 23 to 32 in a very detailed and comprehensive way.

Article 5 of the draft law which aims at regulating sensitive data is another provision that leads to disappointment in the draft since it does not protect sensitive data at all; it just states the conditions under which sensitive data can be processed. In other words the article sets forth the exception without providing the rule itself. On the contrary, article 27 of the Polish Act first sets forth the rule by defining and prohibiting the possessing of personal data and then provides the exceptions in detail.

Article 6 of the draft law is involved with "the rights of the data subject". However the title of the article being "notification of related persons" is quite misleading and does not match with the spirit of the rule. The article corresponding to this one in the Polish Act is article 32 which not only regulates all the rights of the data subject but also sets forth the sanctions or measures that might be applied by the national data protection authority when the rights of data subjects are disrespected. In the last sentence of Article 6 it is indicated that during the transfer of personal data for the purposes of historical, cultural, scientific or statistical purposes and where it is difficult or impossible to satisfy the need to notify the data subject, the

consent of data subject to such a transaction will not be required. When the fact that the kind of research mentioned in article 6 are usually carried out by economical purposes, it can be concluded that for the application of the exemption, public good, as an element of the research, should be taken into consideration as a criteria.

Under Article 7 of the draft law, the request of information on the personal data on them of individuals is made subject to the payment of a price. Getting information on the data about a person is an extension of personality rights and, exercise of personality rights can not be made subject to payments. The corresponding article of Polish Act[477] does not make the exercise of right to information subject to any payment. If the rationale behind foreseeing was prevention of abuse, just the indication that this right shall not be abused by data subjects would be sufficient and the national data protection authority could decide on the alleged abuse considering article 2 of Turkish Civil Code, which requires that the exercise of every right is subject to rule of honesty.

Article 11 of the draft law, sets forth the situations under which exceptions to the general principles for data protection can be provided. According to the Article exceptions can be brought to data protection where the protection of national security, national defense, public interest and security, protection of the rights and freedoms of data subject or others, prevention of crimes, investigations of acts breaching ethical rules of professions or in case the economical interest of the state requires so. However, this article is quite unsubstantiated when the nature of data protection laws which aim at aligning the national laws with EU acquis are considered. As EU Data Protection Directive, only deals with data protection issues in the first pillar, laws[478] aiming at aligning with the Directive are irrelevant with state

[477] See Article 33 of Polish Data Protection Act.

[478] See Polish Data Protection Act as an example.

security issues since they are all related to the third pillar. The Turkish Government has broad authority in intercepting any kind of communications and collecting, processing personal data on citizens but these issues are covered by criminal laws and there is no need to indicate state security issues as exceptions to data protection principles.

In the paragraph (a) of Article 14 of the draft law, it is indicated that in case personal data about the professions of individuals is processed in order to be broadcasted by radio, television or other media, special superior interest of the data filing system owner will be assumed. The paragraph is quite problematic because exceptions should be introduced when a special superior interest of the right owner himself concerned and that interest is linked to the personality rights of the individual. The Polish Act does not have a corresponding article.

Article 15 of the Draft deals with transfer of personal data to third parties. According to the article, the transferor can leave the personal data to a third party if the transferor either has taken guarantees that the transferee will treat the data with same diligence that the transferor might have portrayed or if the transfer has not been forbidden by law. This article is also problematic since the conditions set forth in the article seem to be the alternatives of each other. These two conditions should be satisfied together, if a transfer to third parties will be allowed. Under Polish Act, the consent of the data subject for such a transfer is required[479].

According to Article 18, "personal data that is no longer needed" shall be anonymized, deleted or terminated. It is not possible to understand who does not anymore need the personal data from the wording of the article. Based on the assumption that it is the data filing system operator or the data controller, the article still remains problematic because what should be

[479] See Article 32 of Polish Data Protection Act.

understood from the wording “that is no longer needed” still remains unclear. Under Article 2 of Polish Act, which is the corresponding article, personal data included in the files created specifically for technical, research or education reasons, should be deleted or anonymized after being used by data controllers.

Article 22 of the Draft requires the satisfaction of the conditions of “having worked at least 12 years in public and private sector in positions related to the practice area of the Board” for the election of the members of High Board of Protection of Personal Data. Considering how new and usually how misunderstood the concept of “data protection” in Turkey is, the contrition laid down by law appears to be quite unrealistic.

Election and appointment of Board Members by the Council of Ministers from among the candidates nominated by the Ministries, High Education Board, Turkish Scientific and Technical Research Institute, Ministry of Justice, Association of Turkish Chambers and Stock Exchanges; contradicts with the Article 20 of the draft which indicates that “The board performs its duties independently”. The independence of the Board to the government could be achieved more easily if the Members were elected from candidates nominated also by private sector actors and non governmental organizations or universities.

The indication that the members and president of the Board will continue to perform their original duties together with the duties assigned to them about being a board member is very problematic because it hinders the independency of the board to an important extent. Articles 8 to 23 of the Polish Data Protection Act regulate the establishment, entitlements and responsibilities of Supervisory Authority of Data Protection which sets a sufficient example for an independent national data protection authority.

According to para.3 of Article 26 of the Draft, in case of detection that data protection rules and principles are violated by public entities and institutions, the Board shall ask the related institution or entity to change the way personal data is processed or to stop processing personal data. Furthermore, the Board informs related Ministry Prime Ministry about the situation. Para 4. states that the institutions or entities may refuse to comply with the request of the Board. This article also is quite problematic because whether public institutions or entities will comply with data protection rules totally depends on the decision of the Government and the decisions of the Board are not binding at all. The article contradicts with the independency of the Board. There is no corresponding article in the Polish Act.

- **The Civil Code**

According to Article 24 of Turkish Civil Code, an individual whose personality rights are breached illegitimately has a right to seek for compensation of his/her damages before civil courts[480].

- **The Criminal Code**

Article 132–138 of Turkish Criminal Code regulate the freedom of communication and criminalize the following acts in order to protect personal data:

a) Unlawful recording of personal data: Any person who unlawfully records personal data in sentenced to imprisonment from six months to three years.

b) Unlawful delivery of acquisition of data: Any person who records, political, philosophical, religious inclinations, racial origins, ethical tendencies, health conditions or connections with trade unions of an

[480] See Article 24 of Turkish Civil Code.

individual is also sentenced to imprisonment from six months to three years.

c) Failure to destroy the data within a prescribed period: Any person who is responsible for keeping the data within a defined system is sentenced to imprisonment from six months to one year if he doesn't destroy the data despite expiry of legally prescribed period.

- **The Electronic Signature Code**

According to this law, electronic certificate service providers should abide by the following rules concerning data protection[481]:

a) The electronic certificate service provider may gather personal data only to the degree that it is essential for the reasons of proceeding a certificate. Distribution of personal data to third parties is allowed only with the permission of the data subject whose personal data is being processed;

b) The electronic certificate service provider shall not reveal the certificate to third parties without the permission of the certificate owner; and,

c) The electronic certificate service provider has to inhibit third parties from gathering personal data without the written permission of the data subject. The electronic certificate service provider shall not distribute data without permission of the data subject[482].

- **Turkish Labor Code**

[481] See Article 12 of Turkish Electronic Signiture Code.

[482] See Article 12 of Turkish Electronic Signiture Code.

According to Article 75 of Turkish Labor Code, the employer has to process the personal data of its employees complying with the legislation and the rule of good faith, and not to reveal any such personal data if the employee in question has a justifiable interest in the confidentiality of such data[483].

It is clear that the Code treats personal data of the employee as if it belonged to the employer and searches for a justifiable interest for protection of such data.

- **The Banking Code**

Under Article 73 of Turkish Banking Code managerial stuff and other employees of banks are obliged to keep personal data on their customers confidential[484]. According to Article 159 of Code, breach of such obligation is an act criminalized, commitment of which requires imprisonment from 1 to 3 years and also administrative penalty in money[485]. If such breach is performed for the sake of gaining a benefit, the penalty shall be increased by one sixth.

- **Bank Cards and Credit Cards Code**

According to Article 23 of the Bank Cards and Credit Cards Code, subscribed shops cannot process, reserve or copy the personal data on their customers, which they attain in the pursuit of payment cards in their place, without written permission of the customer concerned[486]. The entities that provide cards are also obliged to keep personal data confidential except for the cases of marketing their own services. Under Article 39 of the Code whoever breaches these obligations will

[483] See Article 75 of Turkish Labour Code.

[484] See Article 73 of Turkish Banking Code.

[485] See Article 159 of Turkish Banking Code.

[486] See Article 23 of Turkish Bank Cards and Credit Cards Code.

be sentenced to imprisonment from 1 to 3 years and an administrative penalty in money[487].

- **Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector**

The regulation prohibits the interception, recording, storage, interruption of telecommunications by third parties without the consent of the parties to that telecommunication, except where it is allowed by law or a court decision[488].

If the subscriber or the user permits the use of his/her personal data for the purposes of marketing the service or performing value added services, the operator is allowed to process the personal data for these services or marketing purposes within the specified time and scope. The subscribers of the users can any time cancel their permission for the processing of data on them. The operator has to inform the subscribers about the personal data processed and the duration of such processing[489].

Traffic data can only be processed by people who are under the authority of the operator and at the same time work for the billing, customer services, fraud and electronic communications marketing or value added services departments[490].

[487] See Article 39 of Turkish Bank Cards and Credit Cards Code.

[488] See Article 8 of Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector.

[489] See Article 9 of Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector.

[490] See Article 10 of Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector.

Traffic data can be shared with natural or legal persons who are responsible for the solution of the conflicts concerning traffic data, interconnection, billing and similar services[491].

Location data of the subscribers or users can only be processed where such data is anonymized or for the performance of value added services where the subscriber did not make an application for the contrary[492].
Operators must inform subscribers about the type of location data or on issues like whether the data will be transferred to a third party or be used for the performance of value added services. Subscribers can any time apply to stop the processing of location data on them[493].

Operators can not use automated communications services that can function needless of human conduct, like faxes, e-mail or short messages services for the purposes of political propaganda[494].

In case the automated communication systems are used for the purposes of direct marketing, the subscribers should be provided with the chance to refuse each message they receive in a simple way. If the subscriber wishes so unsolicited communications, initiated for the purposes of direct marketing and which hide the sender or does not include which address to apply to end the communication held by e-mail, must be prevented[495].

[491] See Article 11 of Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector.

[492] See Article 15 of Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector.

[493] İbid.

[494] See Article 20 of Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector.

[495] See Article 20 of Regulation on the Processing of Personal Data and Protection of Confidentiality in the Telecommunications Sector.

5.2.2. Legislative Framework of Copyright in Turkey

The main Copyright instrument of Turkish Legislation is Law No. 5846 of 5.12.1951.

The law provides exclusive rights for authors[496] and owners of neighboring rights[497] like the performers, phonogram producers, radios, televisions and film producers.

The exclusive rights granted by Turkish Copyright Law can be summarized as the rights to modification, reproduction, circulation, performance, sale and communication to public[498]. Almost the same exclusive rights are provided to the owners of neighboring rights however the law has defined the details of the rights considering the specific nature of the subject of that right[499].

Copyrighted works submitted as proof to the courts, photographs reproduced or circulated by public authorities[500], legislative documents officially published[501], speeches carried out in Grand National Assembly, performance of published works at schools with the indication of the name of the author[502], creation of selected works from published works of art for educational purposes[503], as exemptions of exclusive rights of right holders.

[496] See Article 20 of Law no: 5846.

[497] See Article 80 of Law no: 5846.

[498] See Article 20 of Law no: 5846.

[499] See Article 20 of Law no: 5846.

[500] See Article 30 of Law no: 5846.

[501] See Article 31 of Law no: 5846.

[502] See Article 32 of Law no: 5846.

[503] See Article 34 of Law no: 5846.

Quotations of small passages of a published work for the purposes of personal and independent research or literary study are allowed under the law. Accordingly, incorporations of different components of published musical works in a composition, reproductions of paintings which are made public, using images of works of fine arts for educational purposes are also permitted[504]. Furthermore, daily news published by press or radios can be quoted without restriction by law[505].

The reproduction of copyrighted works for personal use is allowed[506]. Reproduction of a computer program is also allowed where such reproduction is necessary for the use or correction of it[507]. Reproduction of works of fine arts by photography or drawing is allowed if such works are placed on public places, publicly exhibited or sold by auction[508].

Law no 5846 does not define copyright violation. However, the acts that violate copyright are regulated in the law from article 71 to 73.

Article 67 of the Law covers violation of immaterial rights of the copyright holder. If a work is shared with third parties before its publication, the copyright holder can ask the court to take necessary measures to cease the violation. The same rule applies if the name of the right holder has been used on the work without his/her permission.

The right holder may ask for the following if the work has been altered illegitimately:

[504] See Article 35 of Law no: 5846.

[505] See Article 36 of Law no: 5846.

[506] See Article 38 of Law no: 5846.

[507] Ìbid.

[508] See Article 40 of Law no: 5846.

- Cessation of the alleged reproduction, making public, performance or broadcasting by radio of the altered work and collection of the altered copies or their restoration back to their original.

- When a work of fine arts is altered, the right holder can search for the declaration that the change on the work has not been performed by him. Alternatively, he may ask the deletion of his name from altered original[509].

Article 68 involves with the violation of material rights of copyright holders.

- In case a work has been translated without the consent of the author, has been published in breach of the related contract or reproduced in more copies than agreed pursuant to the contract or has been modified or broadcasted or performed to the public, the author can search for the compensation of his damages.[510]

- If copies of a work has been reproduced without the consent of the author but has not been sold yet, the author can claim the destruction of reproduced copies or that the copies be given to him or a compensation[511].

- As compensation the author can claim anything that he might have demanded under a contract if he had a chance to conclude it[512].

An author whose immaterial or material rights are in danger of being violated may ask from the court the prevention of the possible violation. The

[509] See Article 67 of Law no: 5846.

[510] See Article 68 of Law no: 5846.

[511] İbid.

[512] İbid.

author also can search for prevention in cases where the danger is continuous and it is likely that it might happen again[513].

The author whose immaterial rights have been violated may search for compensation of his immaterial damages before the court. The author can also claim for material damages if his material rights are violated according to the general provisions governing torts. Furthermore the author can claim the profits gained due to the violation however the amount claimed under Article 68 will be deducted[514].

Under the law the following acts are subject to imprisonment from 1 year to 5 years or a judicial penalty in money:

- Violation of copyright,
- Selling, renting, lending, circulating the illegitimate copies of a work,
- Buying the illegitimate copies of a work for commercial reasons,
- Alteration of a work without the consent of the right holder[515].

Making quotations without referring to the work and stating the name of the author is subject to imprisonment from 6 months to 2 years or judicial penalty in money.

Following acts are subject to imprisonment up to 6 months:

- Disclosing the text of a work which has not been published yet,
- Referring the source of a work incorrectly[516].

[513] See Article 69 of Law no: 5846.

[514] See Article 69 of Law no: 5846.

[515] See Article 71 of Law no: 5846.

[516] Ibid.

The distribution of the works in violation of the banderole is subject to imprisonment from 1 year to 5 years. Again buying work without banderole or against banderole rules for commercial reasons is subject to the same punishment.

Selling legitimate copies of works with banderoles on them in open air shops is subject to administrative penalties in money. The production of unlawful banderoles is subject to imprisonment from 3 years to 7 years[517].

The law prohibits and criminalizes the circumvention of Digital Rights Management Systems only with regard to computer programmers. According to the law, the manufacture or sale of technical tools that circumvent computer programmes will be subject to imprisonment from 6 months to 2 years[518].

5.3. Implications of DRMs on Turkey

DRM writes and enforces its own copyright law meaning that sometimes DRM systems may enforce more stringent rules than the local copyright laws. What makes it more detrimental is that it dictates the standards of developed countries to the rest of the world.

DRM systems are licensed by big companies which are very powerful in the world market and they function using patents and secrets all around the world. In case local artists are dictated to use DRMs they become dependent to these powerful companies and these powerful companies start to determine the terms and conditions for the distribution of works of art. The big companies can charge a fee over the use of DRMs in this case, thus the

[517] See Article 81 of Law no: 5846.

[518] See Article 72 of Law no: 5846.

Money of artists in developing countries goes to the giant companies of developed countries.[519]

For the development of countries usage of second hand products are quite important because they are low cost and they prevent waste. Used books or other educational tools are significant contributors to the development of anions around world. However, DRM often renders the second hand use of the product impossible by imposing technical restrictions. Such a restriction may be a problem in the developed world but it is an obstacle before the development for developing countries.[520]

DRM systems are not only implemented to copyrighted works but some licensing companies also implement DRM to works that belong to the public. DRM can be implemented to books or movies that are in the public domain. The implementation of DRM to public domain is a danger for the developing countries since it hiders a resource for development. [521]

DRM implemented works end up being sold in the developing countries last after they are submitted to the developed world because of a framework included in the DRMs that is called region windowing. The use of this framework is based on the idea that if goods enter to the market of developing countries at a lower price, they will be resold to the developed countries. Because of this approach the developing countries become last to reach even to literary works[522].

[519]See, Digital Rights Management, a faliure in the developed world, a danger to the developing world, for the International Telecommunications Union, ITU-R Working Party 6M Report on Content Protection Technologies

[520] Digital Rights Management, a faliure in the developed world, a danger to the developing world, for the International Telecommunications Union, ITU-R Working Party 6M Report on Content Protection Technologies

[521] ibid.

[522] ibid.

Since distance education is cheaper than on-campus education it is beneficial for the development of countries. However DRM can hinder also distance learning by prohibiting recording or transferring the content for educational purposes. DRM also will market the second hand use of education tools and some schools may need to rebuy every teaching material for every use and every educational term. This increases the costs of education and undermines development.[523]

DRM also affects the innovation programs of developing countries in a negative sense. Developing countries need technology and law to promote innovation. However the use of DRM advantages the big market players and makes the entry into market very difficult for small actors[524].

Furthermore DRM makes working very difficult for libraries and schools[525].

In most of the countries, local industries have been convinced by DRM licensing companies and international media cartels that DRM is vital for their future existence, turning every actor in the sector a customer of DRM systems[526].

In the 1980s DRM frameworks were used by almost every technology company. They were sure that customers were cheats ready to rob them of all their revenue so they applied more and more stringent restrictions on their products. However, what brought their end was not the illegitimate copying performed by customers but was Microsoft which attained control of 97 percent of the market at that time. Today, Microsoft as a DRM

[523] ibid.

[524] Ress, Manon, DRM and Developing Countries, Washington DC, USA, 29.04.2005.

[525] ibid.

[526] EFF, Digital Rights Management, a faliure in the developed world, a danger to the developing world, for the International Telecommunications Union, ITU-R Working Party 6M Report on Content Protection Technologies

supplier is telling all the sector actors that they will get destroyed if they do not follow the actions of their customers by employing DRMs. [527]

DRM assumes that the public is ready to cheat if they are allowed. DRM is employed to make people act with honesty and be restricted with the actions allowed by rights holders. But these restrictions don't work because the protection provided by DRM is based on making the functioning of the system a secret for the user. However the secret is usually revealed by hackers and the circumvention tools are shared on the internet.

For the development of countries, education and availability of information is vital. This requires the non-profit use and distribution of information products being easier and freer. Some governments and institutions adopting a "copyleft" its approach allowed for noncommercial improvement, re-use and sharing of information goods through free silence schemes[528].

The Massachusetts Institute of Technology (MIT) has shared all of its educational texts in the internet under a Creative Commons license that can be accessed by researchers around the world.[529]

Instead of supporting DRM, culture and arts can be developed through free licensing and customers can escape from Hollywood's attitude towards them and developing nations can be free from the colonization created through the use of DRM.[530]

[527] ibid.

[528] ibid.

[529]EFF, Digital Rights Management, a faliure in the developed world, a danger to the developing world, for the International Telecommunications Union, ITU-R Working Party 6M Report on Content Protection Technologies

[530] ibid.

5.5. Importance of Privacy Laws in Turkey

A life is considered more private when it is either searched or monitored less[531]. For example when someone walks on the streets he is monitored by other people and his life can be searched if he has recorded it in letters or diaries.

The level of monitoring and searching of other people's life is higher in more traditional and less developed countries. In such countries, especially in small towns, almost everybody monitors the life of others. They monitor what others do, how they do it, when they do it etc. Thus in more traditional societies the lives of people are more public and less private. The monitoring of other peoples life makes social control easier.

Up to the digital age what made privacy possible in traditional societies of developing countries were the walls of the houses that separated people from each other. Since those walls were also where the properties of one began, it was only possible to search inside of those walls, under certain circumstances by the police.

However developments in technology have changed the balance of privacy that existed in the analogue world. And this change in the balance required laws to rebalance privacy.

In developed countries especially in the EU where people have a stronger sense of privacy and a history of privacy laws, the gap has been filled with data protection laws and privacy has rebalanced.

The development of technology has been the death of privacy in traditional societies of developing countries. These kinds of societies where people had

[531] Lessing Lawrence, The Architecture of Privacy, Taipei, March, 1998, p:1.

a tendency to collect data on each other more, now had technologies that also do the same data collection service, with the difference that the collection and monitoring performed by these services are not temporary any more.

In the developed world it can be argued that enforcement of data protection is a paternalistic approach and people don't need governments to take measures to protect their privacy. The same argument does not apply to more traditional societies.

In the April of 2010, newspapers reported that 2-3 year old babies were raped and killed by nine 15 year old school boys in a small town in Siirt, Turkey. People were in shock. The details of the story was revealing that these boys that committed the crimes provided babies through their 15 year old cousin, a girl at the same school with these boys. This small town is a very traditional and normative society where not only every action of other people is monitored, but they are also published by the society itself. The boys have forcefully taken the naked pictures of the girl and then have threatened her to make the pictures public if she does not bring them babies. The girl could not complain about the pictures to anyone, because in a society like that people can even kill girls if they are pictured in that way. Thus the pictures, the data of the girl can turn into a life and death issue. The girl with such a fear has taken two children to the boys and the boys after having raped the children have killed them.

The story is the most extreme example of what development of technology without the implementation of necessary laws, in the lack of education can lead to. 15 year old boys can watch child pornography in the internet, normalize any kind of crime, they can blackmail school mates by taking their naked pictures and they can kill 2-3 year old babies by raping with the help of technology.

To conclude it can not be a paternalistic attitude enforces data protection laws in societies like Turkey and it can not be deemed luxurious to educate people of the importance of data protection. Because it is quite clear that data protection can save lives in highly traditional societies.

CHAPTER 6

CONCLUSIONS

In the beginning of 5th Chapter the observation that Turkey has been one of the best markets for the employment of DRMs has been made. This observation was based on the big young population of Turkey, together with the widespread piracy and the lack of a data protection law.

Since piracy has been widespread it has been easier for DRMs suppliers to argue that such systems are needed in especially markets like Turkey. The big young population of Turkey makes it an attractive market for copyright industries and the lack of data protection law and privacy restrictions made the employment of DRMs in Turkish market easier.

However in a dynamic and developing country like Turkey, DRMs like systems have very dangerous consequences. Human resources are one of the most important elements that will contribute to the development of Turkey. How much the educated people might add to the economic growth is not debatable when a country like Turkey is concerned. First of all, DRMs is an obstacle to Turkey's educating its young population by imposing serious restrictions on the access to information. DRMs censor the information and lock away the instruments for development.

DRMs systems employed go beyond the scope of Turkish Copyright Legislation and restrict also the legitimate acts, which fall within the scope of fair use. For example under article 38 of Law on Intellectual and Artistic Works the reproduction of artistic works or computer programs for personal use is not prohibited. But the DRMs systems may render the personal use of the copyrighted work impossible by setting great restrictions. In other

words, Turkish Copyright law grants exclusive rights to copy or distribute to copyright holders, but employing DRMs they extend these rights to such a degree that they can control every single act of the customer. For example if someone buys a book from a book shop, the author does not have a right to monitor or surveil how the book is used, whether the book is read three times or ten times, whether it is copied for personal use of lended to a friend. In case of DRMs, how many times a book can be read, whether it can be copied or not, is it possible to lend it or not is determined by the license.

It is possible to argue that DRMs are as sophisticated agents and spies as James Bond but they are not famous of that since people in developing countries are quite misinformed about their capabilities. The Sony Rootkit incident has proved that through using DRMs it is possible to install spywares to the computers of the customers and this kind of spyware not only monitor the actions of customers violating their privacy but also hinder the security of their computers and lead them become vulnerable to attacks or viruses. Thus each ordinary Turkish family can be watched by several big brothers and their numerous agents just through the computer games, DVDs, computer programs in their households.

As indicated in the previous chapters, under the EU Copyright Directive Member States are to take necessary measures to protect DRMs systems against circumvention. Turkish Copyright Law prohibits and criminalizes the circumvention of Digital Rights Management Systems only with regard to computer programs. However even in official documents neither EU institutions nor Turkish counterparts make any comments on the dark side of DRMs. Most surprisingly even academic studies carried out as consultation to Turkish Culture and Tourism Ministry deal with the

functioning of DRMs or the rules and procedures governing them[532] without the slightest hint on their dangers. It is clear that developed countries act with the assumption that developing countries share the same concerns and needs they do and they do not even think that what works for them may not work for poorer countries or what is beneficial for them can be detrimental for developing countries.

In case of DRMs it is quite clear that Turkey should not be coerced to protect systems that goes beyond national copyright laws and should not sacrifice the legitimate access to information for the protection of technological tools that dictate the control of giant companies on the legitimately acquired works. Turkey should distinguish copyright protection and protection of DRMs from each other and while a balanced copyright system should be promoted, application of DRMs should be discouraged.

Consumer organizations and other non governmental organizations should take necessary steps in Turkey to inform people about the negative affects of DRMs, librarians should be educated on problems concerning DRMs and the government should be lobbied. NGOs should be more proactive in the international field and declare the side affects of DRMs for developing countries before international organizations like World Trade Organization.

As for data protection issues, the review of Draft Turkish Data Protection Law[533] discloses that one of the reasons behind the non adoption of the draft law is quite related to the legislators confusion of first pillar and third pillar data protection and the governments unwillingness to surrender the large extent of data processing enjoyed by public entities.

[532] İstanbul Bilgi Üniversitesi, Bilişim Teknolojisi Hukuku Uygulama ve Araştırma Merkezi, Sayısal Haklar Yönetimi (DRM), İstanbul, 2006.

[533] See pages 72-77 of this thesis for a review.

It is possible to argue that the importance of privacy and the benefits of privacy for individual or the society are not yet quite brought to the coconsciousness by Turkish policy makers.

The benefits of privacy to individuals are not that much esteemed since the importance of self-realization is not yet comprehended in depth. In sociological and physiological terms it is possible to argue that it is impossible for a person to become a self-realized individual and get "in-dividuated" without having enough space between his fellow creatures and him. Privacy and data protection rules aim at protecting the autonomy, self esteem, identity, individuality, dignity, emotional integrity, peace of mind and soul of natural persons.

One can argue that according to the hierarchy of needs of Maslow, self-realization is the last step that is needed to be achieved after all social and economical needs of an individual is satisfied. Furthermore one can claim that privacy and data protection issues are luxurious for developing countries and they can be dealt with after the achievement of economical development. However such an argument would be quite ignorant of the fact that human dignity, self-esteem, individuality and anonymity can never be considered as being luxurious and nothing can develop in an environment that restricts or does not allow the personal growth of individuals.

Data protection rules are needed in Turkey to provide more dignity to individuals and to protect it and nothing is that big a price to pay for the preservation of the integrity of a human being.

The government should take the necessary steps to adopt a data protection law. However when considering the shortcomings of the current draft[534], a

[534] See pages 72-77 of this thesis for a review.

new draft should be prepared by consulting the already enacted data protection laws of the newest members of the European. This will allow the legislator to benefit from a comparative law perspective. A clear distinguishment of first pillar and third pillar data protection should be made, and third pillar issues should be removed from the draft. A more independent and less dependent data protection authority should be created.

Human rights organizations and other NGOs should lobby the government for appropriate changes in the legislation that will allow more perfect protection of privacy and human dignity.

GSM operators or internet service providers should educate their personnel on the importance of data protection. The developments in the April of year 2010 in Turkey has showed that even the personnel of the biggest GSM operator in Turkey is quite uneducated on the importance of confidentiality of communications. Since some GSM workers together with a famous retired soccer player, Rıdvan Dilmen, have been prosecuted with the allegation that they formed an organization for the unlawful interception of telecommunications of people. This incident showed that even the employers of telecommunications are quite unaware of the importance of data protection issues. Considering the fact that even such a huge scandal did not cause a big public outcry, it is obvious that people should be more educated on their rights concerning the data on them. And it is also partly the job of NGOs active in the field of Internet Technologies and Telecommunications.

Universities may also consider opening privacy law courses especially to educate young candidate employers of IT and telecommunications or banking and finance sectors or other such sectors that deal with personal data.

BIBLIOGRAPHY

1. Adam D. Moore, Intellectual Property and Information Control, (2001), Transaction Publishers, New Jersey.

2. Alonso Blas, Diana, Fist Pillar and Third Pillar: Need for a common approach on data protection? International Conference "Reinventing Data Protection", 12 and 13 October 2007, Brussels.

3. Article 29 Working Party, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, adapted on (30 May 2002), 5035/01/EN/Final WP 56.

4. Article 29 Working Party, "Privacy on the Internet: A Comprehensive EU Approach to Online Data Protection. (21 November 2000).

5. Article 29 Data Protection Working Party, xxxx/05/EN WP 104, Working document on data protection issues related to intellectual property rights, (18 January 2005).

6. Badvista, "FSF launches campaign against Microsoft Vista", Press Release, http://badvista.fsf.org/blog/launch-press-release, last checked on 20.10.2009.

7. Badvista, "Five ways to help the badvista.org campaign", http://badvista.fsf.o rg/blog/5-ways-to-help-the-badvista-org-campaign,last checked on 20.10.2009.

8. Bainbridge, David, Introduction to Information Technology Law, Six Edition, PearsonLongman, (2007).

9. Bangeman, E., "Tivo Tightens the DRM vise", (28.10.1006), last checked on 26.10.2009.

10. Bergkamp, Lucas, EU Data Protection Policy, The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in An Information-Driven Economy, Computer Law&Securtiy Report, Vol.18, no.1.

11. Bygrave, Lee A, Digital Rights Management and Privacy-Legal Aspects in the European union, in E. Becker et al., Digital Rights Management: Technological, Economic, Legal and Political Aspects, Heidelberg: Springer Verlag, (2003).

12. Bygrave, Lee A, The Technologisation of Copyright: Implications for Privacy and Related Interests, European Intellectual Property Review, (2002), vol.24.

13. Cameron A., Digital Rights Management: Where Copyright and Privacy Collide, Canadian Privacy Law Review, (2004).

14. Carey, Peter, Data Protection, A Practical Guide to UK and EU Law, Oxford University Pres, (2004).

15. Cate FH, Staten ME., Protecting Privacy in the New Millenium: The Fallacy of Opt-in, 2001.

16. Cavoikian A., Information and Privacy Commissioner/Ontario, Privacy and Digital Rights Management: An Oxymoron?, (2002).

17. Center for Democracy and Technology, Evaluating DRM: Building a Marketplace for the Convergent World, (September 2006).

18. CIPPIC Report, Digital Rights Management Technologies and Consumer Privacy, An Assessment of DRM Applications under Canadian Laws, (September 2007).

19. Consolidated version of the Treaty on European Union.

20. COM (90) 314 final-SYN 287, OJ C 277, (05.11.1990).

21. COM (92) 24 final-SYN 393, OJ C 311, (27.11.1992).

22. COM (2004) 61 of (03.02.2004) "Connecting Europe at high speed: recent developments in the sector of electronic communications".

23. Combating Counterfeiting and Piracy in the Single Market-Green Paper, COM (98) 569 Final, Brussels, (15.10.1998).

24. Comments of the Electronic Privacy Information Center (EPIC) and the Information Society Project (ISP) at the Yale Law School on the Public Consultation of the Working Party on the Protection of individuals with Regard to the Processing of Personal Data on Data Protection Issues related to intellectual Property Rights, (31 March 2005).

25. Communication from the Commission the the Council, the European Parlimaent and the Economic and Social Committee, Follow- up to the Green Paper on combating counterfeiting piracy in the Single Market,COM (2000) 789 Final, Brussels, (30.11.2000).

26. Commission Staff Working Document, Report to the Council, the European Parliament and the Economic and Social Committee on the application of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, Brussels, (31.11.2007), SEC(2007) 1556.

27. Commission of the European Communities, Commission Staff Working Paper on Digital Rights, Background, Systems, Assessment, Brussels, 14.02.2002, SEC (2002) 197.

28. Coyle, K.,"The Technology of Rights: Digital Rights Management", (PDF). http://www.kcoyle.net/drm_basics.pdf, (19.11.2003), last checked on 26.10.2009.

29. De Hert, P.& Gutwirth, S., 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E.Claes, A Duff & Gutwırth (eds..), Privacy and the criminal law, Antwerp/Oxford, Intersentia, (2006).

30. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , (23.11.1995) p. 0031 – 0050.

31. 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.)

32. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of

copyright and related rights in the information society, OJ L 167, (22.6.2001).

33. Directive 1997/7/EC of the European Parliament and the Council of 20 May 1997 on the Protection of Consumers in respect of Distance Contracts [1997] OJ L144/19.

34. Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of electronic commerce in the Internal Market [2000] OJ L 178/1.

35. Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures [2000] OJ L13/12.

36. Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights.

37. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, OJ L 77, 27.3.1996.

38. Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

39. Directive 98/84/Ec Of The European Parliament And Of The Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access, Official Journal L 320 , 28/11/1998 p. 0054 – 0057.

40. DRM and Film", http://www.bigurlpro.info/DRM-film.html, last checked on 20.10.2009.

41. EDRI-Gram, "Private copy explained by Court of Appeal in Paris", 12.04.2007, http://www.edri.org/edrigram/number5.7/private-copy-france, last checked at 20.01.2010.

42. European Parliament, The EU's External Relationships, http://www.europarl.europa.eu/parliament/expert/displayFtu.do?language=en&id=74&ftuId=FTU_6.3.2.html, last checked on 25.10.2009.

43. Einhorn, Michael A., Canadian Quandary: Digital Rights Management, Access Protection, and Free Markets, the Progress and Freedom Foundation, Release 13.12. (May 2006).

44. Electronic Frontier Foundation, Who controls your television, PDF available at http://w2.eff.org/IP/DVB/dvb_paper_032007.pdf, last checked on 26.10.2009.

45. Electronic Frontier Foundation, Sony BMG Info, http://www.eff.org/IP/DRM/Sony-BMG/, 2005, last checked on 26.10.2009.

46. Electronic Frontier Foundation, 'An Open Letter to Sony BMG', http://www.eff.org/IP/DRM/Sony-BMG/?=open-letter-2005-11-14.html, 14.10.2005, last checked on 25.10.2009.

47. European Commission, Justice and Home Affairs, Data Protection, Rules of Procedures of Working Party of 18 February 2008, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/rules-art-29_en.pdf, PDF, last checked on 25.10.2009.

48. European Union, How the European Union Works, Your guide to the EU institutions,http://www.avrupa.info.tr/Files/File/Publications-2006/brochures/en-HowEUWorks.pdf, last checked on 25.10.2009.

49. Feigenbaum, J., Freedman, Michael J., Sander, T. and Shostack, A., Privacy Engineering for Digital Rights Management Systems, Computer Science Department, Yale University, 2002

50. Frauenfelder, M., "Amazon zaps purchased copies of Orwell's 1984 and Animal Farm from Kindles". http://boingboing.net/2009/07/17/amazon-zaps-purchase.html, 17.07.2009, last checked on 26.10.2009.

51. Geist, M., 'Sony's Long-term Rootkit CD Woes', BBC News, 21 November 2005.

52. Guarda, Paolo, Data Protection, Information Privacy and Security Measures, An Essay on the European and Italian Legal Frameworks, Version 1.0- December 2008.

53. Halderman, J.A, and Felten, E., 'Lessons from the Sony CD DRM Episode', available at http://itpolicy.princeton.edu/pub/sonydrm-ext.pdf, 14.02.2006, last checked on 26.10.2009.

54. High Level Group on Digital Rights Management, Final Report, March-July 2004.

55. "Internet Music", http://www.bigurlpro.info/internet-music.html, last checked on 20.10.2009.

56. J Lloyd, Ian, Information Technology Law, Oxford University Press, 2004.

57. Kacrorowska, Alina, European Union Law, Routledge.Cavendish, Taylor and Francis Group, London and New York, 2009.

58. Kantor, A., 'Sony: The Rootkit of All Evil?' USA Today, http://www.usatoday.com/tech/columnist/andrewkantor/2005-11-17-sony-rootkit_x.htm, 17.11.2005, last checked on 25.10.2009.

59. Kerr, I. and Bailey J., The Implications of Digital Rights Management for Privacy and Freedom of Expression, Journal of Information, Communication and Ethics in Society, 2004

60. Kuner, Christopher, European Data Privacy Law and Online Business, Oxford University Press, 2003.

61. Lessing, Lawrence, Free Culture, How Big Media Uses Technology and Law to Lockdown Culture and Control Creativity, New York, Penguin, 2004

62. Litan RE., Balancing Costs and Benefits of New Privacy Mandates, AEI-Brookings Joint Center for Regulatory Studies, Working Paper 99-3, April 1999.

63. Maximilliano Santo Cruz S., Intellectual Property Provisions in European Union Trade Agreements, Implications for Developing Countries, ICTSD Intellectual Property and Sustainable Development Series, (June 2007).

64. McGuigan, B., “What is DRM”, http://www.wisegeek.com/what-is-drm.htm, last checked at 26.10.2009., B., “What is DRM”, http://www.wisegeek.com/what-is-drm.htm, last checked at 26.10.2009.

65. Noring, J., "The Perils of DRM Overkill for Large Publishers", http://www.teleread.org/publishersdrm.htm, 2004, last checked on 26.10.2009.

66. New York Times, “Amazon Erases Orwell Books From Kindle Devices", 07.18.2009, last checked on 26.10.2009.

67. Opinion of the European Economic and Social Committee on the ‘Proposal for a Directive of the European Parliament and the European Council on the measures and procedures to ensure the enforcement of intellectual property rights. (OJ C32 of 5.2.2004,15)

68. Opinion 2/2003 on the application of data protection principles to the Whois directories, 10972/03/EN final, WP 76

69. P. Terence, European Intellectual Property Law, Ashgate Dartmouth, 2000.

70. Pogue, D., New York Times, "Some E-Books Are More Equal Than Others", http://pogue.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/, 17.07.2009, last checked on 26.10.2009.

71. Poullet Y., Gutwirth S., The Contribution of the Article 29 Working Party to the construction of a harmonised European data protection system: an illustration of ‘reflexive governance’?, Brussels, 2008.

72. Poullet, Y., Transborder Data Flows and Extraterritoriality: The European Position, Journal of International Commercial Law and Technology, Vol. 2, Issue 3, 2007.

73. Proposal for a Directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights, (6777/03), 06.02.2004, availabte at http://ipjustice.org/CODE/020604EUIPED.html, last checked on 25.10.2009

74. R. Marlin-Bennett, Knowledge Power, Intellectual Property, Information and Privacy, Lynne Rienner Publishers, Inc., 2004

75. Rayna T., Striukova L., Digital Rights Management: White Knight or Trojan Horse, Discussion Paper, Department of Economics University of Bristol, 2007

76. Recommendation 3/97 "Anonymity on the internet", adopted 3.12.1997;Working document: Processing of Personal Data on the Internet, adopted by the Working Party on 23 February 1999, WP 16, 5013/99/EN/final.

77. Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, adopted by the Working Party on 23 February 1999, 5093/98/EN/final, WP 17.

78. Reed, Chris and Angel John, Computer Law, The Law and Regulation of Information Technology, Sixth Eddition, Oxford University Press, 2007.

79. Rimmer, Matthew., Digital Copyright and the Consumer Revolution, Hands off My iPod, Edward Elgar Publishing Limited, 2007

80. Roush, W., 'Inside the Spyware Scandal', Technology Review, 2006

81. Solove, Rotenberg, Schwartz, Information Privacy Law, Apsen Publishers, New York, 2006.

82. Thumm N., Intellectual Property Rights, National Systems and Harmonisation in Europe, Physica- Verlag Heidelberg, 2000, Germany.

83. Translation of the Ruling of Google v Copiepresse, Brussels Court of First Instance , 13th February 2007, available at, http://www.copiepresse.be/13-02-07-jugement-en.pdf., last checked on 20.01.2010.

84. Vrins, O. and Schneider M., Enforcement of Intellectual Property Rights Through Border Measures, Oxford University Pres, 2006.

85. Woelert, L., 'Sony's Escalating "Spyware" Fiasco', Businessweek, 22 November 2005.

86. Xeni Jardin, "Report: HD-DVD copy protection defeated". Boingboing. http://www.boingboing.net/2006/12/28/report-hddvd-copy-pr.html, 28.12. 2006, last checked on 26.10.2009.