Intellectual property versus data protection on the internet

By Dimitra-Georgia Tsiaklagkanou

Intellectual property versus data protection on the internet

Introduction

I. The obligation of electronic communication providers to provide the personal data of internet users

A. The IP address as personal data and as part of communication

B. Matching a user's IP address with a subscriber to an internet connection

II. Obligation to retain data

Concluding remarks

Introduction

- Intellectual property is all around us, i.e. the intellectual property of artists or performers, or the creators of computer programmes
- The internet may provide anonymity and freedom of movement by the user
- However, the act of surfing the internet may leave a huge trail of personal data behind
- Conflict between the protection of intellectual property and of privacy
- Can the creators of works and other rightholders use the identification data of the internet users?
- Greek and French law

I. The obligation of electronic communication providers to provide the personal data of internet users

- A. The IP address as personal data and as part of communication
- The IP address is automatically assigned by a provider of internet access services to any internet user
- However, there is a possibility that the IP address cannot identify the internet user.
- Under ***French*** law, according to some court decisions, the IP address does not constitute personal data information; the IP address *“refers only to a machine and not to the person using it"*
- Other court decisions accept the IP address as personal data, i.e. by stating that “*this address appears to be the only evidence related to the person who posted the published content”*
- No answer from the French Supreme Court (judgement 13.01.2009)

The IP address as personal data

- Article 29 Data Protection Working Party, Opinion 4/2007: *“on the Web, web traffic surveillance tools make it easy to identify the behaviour of a machine and, behind the machine, that of its user”*
- Opinion 2/2002: *“IP addresses attributed to Internet users are personal data”*
- the Decree of 5 March 2010 classifies the IP address among personal data that the HADOPI authority may process in order to send recommendations to internet users.
- The Conseil Constitutionnel, decision no 2009-580
- Within the **Greek** legal system: the IP address as part of communication

The IP address as part of communication

- The Prosecutor's Opinion 9/2009 the communication via internet is *"public communication", "there is no intention of the communicating persons to keep the conversation secret*"
- Prosecutors' Opinions 12/2009 and 9/2011
- By contrast, according to Greek Data Protection Authority, *"The monitoring of employee's e-mail may be considered necessary only in exceptional cases"*
- Assuming the privacy of the communication via telephone, but denying that character in communication via internet, implies discrimination against the internet
- The Directive 2002/58/EC: *"a communication may include any … numbering or addressing information provided by … the user of a connection to carry out the communication"*
- Law 3471/2006, Presidential Decree 47/2005, Opinion of *ΑΔΑΕ* 1/2005
- Judgement Malone and Copland

B. Matching a user's IP address with a subscriber to an internet connection

- 1. The Promusicae case (29.01.2008):
- Community Law does **not** *"require the Member States to lay down, in a situation such as that in the main proceedings,* ***an obligation to communicate personal data*** *in order to ensure effective protection of copyright in the context of civil proceedings"*
- case *LSG-Gesellschaft v Tele2 Telecommunication,* 19.02.2009
- case *Bonnier Audio AB a.o. v Perfect Communication Sweden AB*, 19.04.2012

2. Solutions provided by the Greek and French legal systems

- a. The waiving of confidentiality in the Greek and French legal systems
- Under ***Greek*** *law*, Article 19.1 of the Greek Constitution allows the waiving of confidentiality for reasons of national security or for offences of particular gravity
- Law 3471/2006 Article 3
- Law 2225/1994 Article 4
- Not applicable for violations of the intellectual property

The waiving of confidentiality

- The French Law 91-646 dated 10.07.1991 provides the **waiving of confidentiality** to protect the public interest, such as national security, the protection of important scientific and economic elements of France, the prevention of terrorism, crime and organized crime
- Intellectual property is not included in the scope of this Law
- Article 15.1 of the Directive 2002/58/EC: possible restriction of the right to confidentiality of the communication in order to investigate criminal offences or of unauthorised use of the electronic communication system

b. Processing personal data in the Greek and French legal systems

- Processing data should either be notified, or authorized, by the competent authorities
- Processing of personal data without the data subject's consent: Article 5.2 (e) of the Greek Law 2472/1997
- If *"the processing is absolutely necessary so that the legitimate interests pursued by the controller, or the third party/parties to whom the data are provided, can be satisfied, and on condition that these interests are obviously superior to the rights and interests of the data subjects, and without compromising their* ***fundamental freedoms****"*
- This possibility is not provided by the Article 5.2 of the Law 3471/2006
- Law 78-17 Article 7.5
- However, the communication confidentiality should be considered as a fundamental freedom

Processing personal data

- No overlapping of powers concerning the competent authority for the protection of personal data and the competent authority for the waiving of confidentiality
- The Greek Law 2472/1997 is not applicable to data processing carried out by the courts or prosecutors; however, the provisions of Criminal and Procedure Law are applicable (i.e. the Law 2225/1994) (Article 3.b)
- Under French Law, processing of personal data relating to offenses can be carried out by the courts, or the collecting societies (Article 9 loi 78-17), in respect to other laws, i.e. the law HADOPI
- The processing carried out by the collecting societies should be authorized by the *CNIL* (Article 25.3 loi 78-17)

Imposing technological measures upon a provider

- **Directive 2004/48/EC** (Article 8.1): *"the competent **judicial authorities** may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided **by the … person** who: (c) was found **to be providing on a commercial scale services used in infringing activities**"*
- Articles 63.2 of the Law 2121/1993 and L. 615-5-2 CPI
- **Directive 2000/31/EC** Article 18
- **Article 64 A** of the Greek Law: *"Rightholders **may request an order against intermediaries** whose services are used by a third party to infringe a copyright or related right"*
- CJEU, C-557/07: *"**access providers** which merely provide users with Internet access … must be regarded **as 'intermediaries'***
- **Court of First Instance of Athens**, no 4658/2012 imposed to service providers a filtering obligation regarding specific webpages infringing intellectual property rights

c. Application of the French Law HADOPI

- A duty of care to subscribers of an internet access service, so as to ensure that no acts infringing intellectual property take place through the use of their internet connection
- The **Law HADOPI 1**, no 2009-669,12.06.2009
- The **Law HADOPI 2,** no 2009-1311, 28.10.2009
- Sending letters to subscribers informing them of infringements of intellectual property
- Sending a second letter within six months
- Retention of data by the HADOPI authority for as long as necessary
- *Agents assermentés*, employed by the HADOPI authority, collect the personal data of internet users
- The rightholders may also appoint *agents assermentés* and then either contact the HADOPI authority or appeal to the courts

Application of the French Law HADOPI

- The matching of IP addresses of internet users to internet access service subscribers is carried out by the HADOPI authority
- The rightholders or **collecting societies cannot have access to this data**
- If non-compliance by the subscriber, urgent court proceedings after six months from the second letter sent by the HADOPI authority
- Possible issuance of an order for interruption of internet access service - only **by a judicial authority**

d. Criticisism against the Law HADOPI

- **Directive 2009/140/EC** the interruption of internet access service could only be imposed following to a ***"prior, fair and impartial procedure"***, instead of judicial intervention
- Restrictions on freedom of expression, or exercise of a profession
- The law expressly provides for consideration if professional
- However, professionals should not be treated more favorably than individuals
- **Presumption of guilt** against the subscriber
- Relief of liability by proving to have taken the necessary security measures to avoid such acts or by proving either third party's fraudulent conduct or force majeure
- However, he has not contributed in any way to these infringements of intellectual property
- Reversing the presumption seems extremely difficult
- He has not to prove that he is not himself the offender, but that a third party used deceptively his internet connection

Liability of the subscriber

- The subscriber is **not** liable for intellectual property infringements that **a third person** has committed
- No strict responsibility due to the actions of a third person
- **But subjective liability** for failing to take security measures for his internet connection
- Relief of its liability if he proves no fault
- a **reinforced obligation of means** and not an obligation of result = false (*vóθo*) strict liability under Greek law

Criticisism against the Law HADOPI

- The HADOPI law aims at suppressing file-sharing on networks (P2P)
- Other spreading techniques also exist, i.e. streaming
- In case of interruption of access service, the subscriber still has to pay the fee to the provider
- Discriminating in favour of the provider:

- He takes advantage of this amount
- He is relieved of his liability (Articles 12 and 15 of Directive 2000/31/EC)

e. EDPS and Greek case-law regarding the “three strikes disconnection policies”

- The EDPS has pronounced upon the “**three strikes disconnection policies**” by considering that *“a three strikes Internet disconnection policy constitutes a disproportionate measure*
- **Court of First Instance of Athens** (no 4658/2012): this policy “*should be considered as **incompatible with Greek Law***”
- *The constitutional right includes, inter alia, the claim to have access to infrastructure of the information society*
- *These … technologies … are used for, among others, perfectly legitimate uses*
- In the United Kingdom, the Digital Economy Act 2010 provides a system of gradual notification
- In Germany, no such legal framework
- in France, reexamination of the system following the presidential election on 6 May 2012

II. Obligation to retain data

- 1. The **Directive 2006/24/EC** : data retention for security reasons
- **Directive 2002/58/EC**: retention of subscribers' or users' personal data for as long as necessary <u>for the service charge</u>
- **Directive 2006/24/EC**: data retention for a period of <u>6 months to 2 years</u>
- *Greek* Law 3917/2011: for one year
- Providing subscribers' data to the national authorities under conditions set forth in Law 2225/1994
- Article 5.5 of the Law 3471/2006 as modified by the Law 4070/2012: *"the provider … must … enable the use and payment of these services anonymously or under a pseudonym"*
- Under *French* law, data retention for one year (Articles R. 10-13 and L. 34-1-III of CPCE) and

  the retained data **can be used for intellectual property protection**

Obligation to retain data

- German Constitutional Court, interim judgement of 11.03.2008: the use of data can only be made in judicial proceedings in progress for a particular serious violation
- Judgement of 2.03.2010: *"a duty of storage … is not automatically unconstitutional at the outset"* , but should respect the principle of proportionality
- Data retention obligation not applicable to search engines
- Article 29 Data Protection Party in the Opinion 1/2008: maintaining data for 6 months

2. Article 6-II and 6-III of the French Law 2004-575

- **Article 6-II** of the French Law 2004-575: providers should maintain data of users who **contribute in creating content** published on a website
- The providers may have to communicate this data to a judicial authority
- Article 6-III gives a list of data which persons with a professional activity as a content editor should make available to the public
- Individuals may retain anonymity
- Which personal data the providers had to demand from users and maintain?
- Is the IP address sufficient?
- Should the provider confirm data provided by a user?

Decree 2011-219

- Decree 2011-219 listed personal data to be maintained
- Including:
- the bank reference of the payment as well as the payment amount regarding a paid e-service
- the password access to electronic services
- Data retention period for 1 year
- Provision to cover the excessive cost of providers due to data retention obligation
- **Decision of the *Conseil Constitionnel*** 2000-441:

"*requiring operators … and to contribute in safeguarding the public order … is outside the scope of the operation of telecommunications networks; therefore, the operators should **not** cover directly the above resulting costs*"

3. LOPPSI 2: data retention for strengthening national security

- French **Law 2011-267** enables remote access to a user’s computer for detection of certain crimes, if allowed by a judge
- Not applicable to intellectual property infingements
- German Constitutional Court, judgement of 27.02.2008: refused to allow the remote access to a user's computer

➔The retention and the subsequent processing of personal data has become the rule

Concluding remarks

- The protection of intellectual property is **in conflict** with:
- the protection of **privacy**
- the protection of **personal data**
- the **freedom of expression**
- the **confidentiality** of the communication

➔The result of the conflict is left to be resolved by the national regulators

➔Principles of proportionality and of necessity

Concluding remarks

- Under Greek Law, no waiving of confidentiality for intellectual property infringements

➔ Disclosure of the users' data **is <u>not</u> allowed** under any circumstances

- Under French law, courts and collecting societies can process data regarding to offences, in respect to other laws; the HADOPI authority **may process users' data** in order to send letters to subscribers

➔ The rightholders have no access to users' data without judicial intervention

➔ Users' privacy is adequately protected

No conflict

- Areas whereby conflict does not exist:

i) works available with licenses Creative Commons

- licensed CC works can be exchanged via file-sharing networks

ii) open source software:

- the use of works is in accordance with the conditions laid down therein

Reconciliation of intellectual property and personal data protection

- Signing agreements with platforms on which their works are available in exchange for a fee
- The interests of rightholders:
- they receive remuneration
- they benefit from greater visibility of their works to a wider audience
- The interests of the platforms:
- they provide richer content to the public
- increased revenue from advertising
- platforms are exempted from liability for intellectual property infringement
- However, an agreement of related rights holders is also required

No general filtering obligation. Users' education. Technological measures. Global license.

- CJEU, C-70/10, *Scarlet Extended v SABAM,* 24.11.201: a general filtering obligation cannot be imposed on service providers
- CJEU, C-324/09, *L'Oréal v eBay International,* 12.07.2011: no obligation of active monitoring of all the data
- Education of users so as to respect others' rights, i.e. the letters sent by the HADOPI authority, educational messages on websites
- Filtering content on a website by using methods as digital watermarking, audio or image fingerprints, i.e. technology "Audible Magic" used by MySpace and Facebook, "Signature" technology by Dailymotion, "content ID" by YouTube
- Use of technological measures designed to prevent or restrict not authorised acts if processing of personal data is carried out in compliance with Directive 95/46/EC (Paragraph 57, Preamble to the Directive 2002/29/EC)
- A system of "global license" was rejected

Exemption for private use. ACTA.

- **The exemption for private use** not accepted by the case-law
- The exemption of private copying cannot result in making legal the reproduction of an illegally acquired work
- The exemption does not meet the requirements of the three step test
- **ACTA**: Anti-Counterfeiting Trade Agreement
- States may require providers to disclose the personal data of copyright or related rights infringers
- Not providing explicitly for exceptions that should be considered as fair use
- The approval of ACTA by the European Parliament is pending

SOPA, PIPA

- U.S. Congress seems to abandon because of the reactions:
- **SOPA** (Stop Online Piracy Act) and
- **PIPA** (Protect Intellectual Property Act)
- The Ministry of Justice could publish black lists of problematic websites and could command internet service providers to block access to these sites
- Rightholders could demand that the providers take preventive measures upon a simple notification. No liability of the providers for blocking innocent sites.

ACTA

- The digital agenda commissioner Neelie Kroes admitted *“We are now likely to be in a world without the [stalled US act] SOPA and without ACTA. Now we need to find solutions to make the internet a place of freedom, openness, and innovation fit for all citizens, not just for the techno avant-garde”*
- Condition of freedom, openness, and innovation is the protection of users’ privacy