

Markt/2006/09/E
Service Contract ETD/2006/IM/E2/69

**STUDY ON THE LIABILITY OF
INTERNET INTERMEDIARIES**

COUNTRY REPORT – Greece

Executive summary

November 12th, 2007

By Giovanni Maria Riccio, University of Salerno (Italy)

Part 1: Legislation

ECD was implemented in Greece by the Presidential Decree No. 131/2003 [Government Gazette (FEK) A 116/16-5-2003] “Implementation of Directive 2000/31 of the European Parliament and of the Council on certain aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) [hereafter PD 131/2003], that came into effect on January 17th, 2002.

Paras. 1, 2 and 3 of article 11 PD 131/2003 have implemented verbatim article 12, paras. 1, 2 and 3 ECD.

Similarly, article 12 PD 131/2003 has implemented verbatim article 13 ECD.

Article 13 PD 131/2003 has implemented almost verbatim article 14 ECD besides the reference to notice and take-down procedures in 14 para. 2 ECD, that is absent in the Greek regulation.

Article 14 para. 1 PD 131/2003 has implemented verbatim article 15 para. 1 ECD.

Article 14 para. 2 PD 131/2003 has implemented almost verbatim article 15 para. 2 ECD by imposing to the providers the duty to inform the competent public authorities of alleged illegal activities promptly. However, the Greek regulation includes a general reservation to the protection of secrecy and of personal data (“Notwithstanding the protection of secrecy and of personal data the information society service providers are obliged to inform immediately ...”).

These provisions are considered to exempt the ISPs from every liability (civil, penal, administrative) even the severe liability of service providers according to article 8 of the Law 2251/1994 on consumer protection. One considerable exemption to the no-liability rule is the field of data protection. Data Protection Rules are generally exempted from the application field of PD 131/2003 (article 20 para. 1 (b) PD 131/2003, article 1 para. 5 (b) ECD).

1. Although Greece has special legislation on specific illegal (off- and on-line) activities (illegal gambling, child pornography, terrorism etc.) there are no provisions imposing specific duties and obligations on ISPs. ISPs may theoretically be considered as perpetrators or accomplices of specific crimes described in the above mentioned legislation but it is indisputable that they can generally defend themselves with the exemptions of articles 11-13 of the PD 131/2003 (12-14 ECD).

Part 2: National Case Law

The search for relevant authority resulted having extremely few judicial precedents (among the published decisions) and no more than five scientific publications based on experience from foreign jurisdictions. Thus, relevant Case Law in Greece is practically inexistent even on the level of First Instance Courts.

1. First Instance Court of Athens, dec. no 1639/2001:

Application for interim measures against an internet user and his ISP for the termination of the infringement of the intellectual property rights and violation of the applicant's professional reputation and personality. The user has set up a website in which he placed without the applicant's previous consent extracts from the content of the applicant's book and a presentation of her CV, publishing her name and picture amongst other obscene pictures, referring in an offensive way to the applicant, doubting the truth of the content of the applicant's CV, creating an email address which he presented as being the applicant's fan club email address. The application was found admissible against both the user and the ISP, however it was upheld only against the user on the merits of the case, since the ISP had already disabled access to the user's website. The case was decided before the implementation of the Directive 2000/31/EC and it does not refer to its provisions regarding the liability of intermediaries.

2. The 'blogme.gr' case:

In a recent notable case the administrator of a Greek information and RSS-based news aggregation website (<www.blogme.gr>) faced criminal prosecution for a blog entry that appeared on his webpage allegedly originating from an other blog ('FunEL-Blog'). 'FunEL-Blog' allegedly satirized a public person residing in Greece, who sued for Slander in Greece. According to the prosecuted administrator 'FunEL-Blog' is hosted in the U.S.A. and its administrator resides abroad, whereas the administrator of the Blogme.gr-webpage allegedly restricted himself to register in its directory and in the RSS flow a link to 'FunEL-Blog', without preserving any slanderous content in his server. Police arrested the administrator and confiscated part of his equipment and the public prosecutor prosecuted him for slander. This questionable case yielded public reaction in the small community of Greek bloggers and the Minister of Public Security had to give explanations in the Greek Parliament [Paper Nr. 7017/4/6575/24-11-2006 of the Ministry]. The case has not been decided by a court yet.

3. Not directly relevant is the First Instance Court of Athens, dec. no 2110/2002:

Application for interim measures of an internet user against his ISP for the blocking of his outgoing e-mails because of alleged spam activity. The application was dismissed, on the grounds that the applicant had offended the Law 2472/1997 on data protection and the terms of his contract with the ISP.

4. Irrelevant are cases concerning the awarding of domain names (cf. First Instance Court of Athens, dec. no 1554/2002).

This scarcity is not to be explained through the existence of the exemption rules of articles 11-14 PD 131/2003 but rather by the statistically proven limited expansion of internet-use among the Greek population.

Part 3: Notice and take down procedures

A. Regulation

Formalised notice and take down (hereinafter: NTD) procedures are not regulated in Greek Law nor implemented broadly. To our knowledge, there are no official bills or any legislative or self-regulative initiatives for the introduction of NTD procedures despite article 16 ECD that has been transposed verbatim into Greek Law.

B. Self-regulation

ISPs have allegedly drawn and implemented on the individual initiative procedures to remove or disable access to illegal or infringing information [among other reasons in order to comply with article 13 para. 1 (b) PD 131/2003 (article 14 para. 1 (b) ECD)]. They are, however, reluctant to divulge any specific information, as the structure and the internal operation of these procedures are considered by the ISP's as business secrets. On the other hand, most ISPs on individual initiative provide in the terms and conditions of the contracts concluded between them and their clients, that they are entitled without limitation to remove or disable access to every information, alleged to be illegal or infringing, after prior notification of the client, even without his consent (it is however questionable, whether such clauses may be considered as unfair and thus void). There is no coordination between the ISPs, initiated by a public authority or by their own organisations, so that the internal NTD procedures base on an individual interpretation of the various legal provisions.

C. Co-regulation

There are no general or specific self- or co-regulatory provisions or business internal codes of contact. The Greek Data Protection Agency has attempted to draft a Code of Conduct concerning Spam without any published results yet. In the field of Intellectual Property no initiative has become public concerning self- or co-regulatory measures, although there are many active collective societies.

Despite this, many service providers have launched and implemented monitoring procedures and technical automatic filtering measures (especially in relation to spam) in order to prevent the abuse of their services and infrastructure from abusive and/or illegal behaviour especially in respect of data protection and data security. Indeed, every ISP is obliged to implement a general Security Policy, which amongst other things includes an Acceptable Use Policy (AUP) of the ISP's products and services. Such policies usually contain antispamming and antivirus policies, as well as individual provisions relating to the information and content transmitted by the recipient of their services through the use of the providers' communications networks and services.