SABAM v. Netlog (CJEU C 360/10) … as expected!

Kluwer Copyright Blog
February 20, 2012

Philippe Laurent (Marx, Van Ranst, Vermeersch & Partners)

Please refer to this post as: Philippe Laurent, 'SABAM v. Netlog (CJEU C 360/10) … as expected!', Kluwer Copyright Blog, February 20 2012, http://copyrightblog.kluweriplaw.com/2012/02/20/sabam-v-netlog-cjeu-c-36010-as-expected/

The CJEU's ruling in the Scarlet v. SABAM case (C 70/10) is still fresh in our memories: court injunctions to install global and preventative filtering systems with a view to preventing copyright infringements are precluded. SABAM asked again for the same measures in the framework of the SABAM v. Netlog litigation. Again, the Belgian court referred the question to the CJEU for a preliminary ruling. Again, the CJEU repeated *mutatis mutandis* its reasoning and reached the same conclusion (C 360/10). *Bis repetetita placent*?
Not exactly: whereas Scarlet is an ISP, Netlog is a Facebook-like online social network. This brings along several factual differences which could have had consequences as regards the application of the law. On the one hand, ISPs transmit information in communication networks and provide access to these networks. They do no not store information (unless temporarily for transmission efficiency only) and are "mere conduits" as regulated by article 12 of the E-Commerce Directive 2000/31/EC. On the other hand, as stated in §27 of the commented decision, Netlog is a hosting service within the meaning of article 14 of Directive 2000/31 in that it owns a social networking platform and stores information provided by the users on its servers. From a technical perspective, filtering communications (data transmissions) in a network is very different from scanning one's own servers content (data storage)…

However, article 15 of Directive 2000/31/EC, which provides for a prohibition to impose a general obligation on providers to monitor the information which they transmit or store, does not make any distinction between ISPs and hosting services providers. Likewise, the CJEU does not seem to have taken the technical distinction into consideration, and has therefore issued a quasi-identical decision. The similitude between the two decisions is striking, as the whole part outlining the considerations of the Court has been literally copy-pasted from the Scarlet v. SABAM decision.

So what can be said about this new decision that has not already been commented as regards Scarlet v. SABAM? Not much really, except the factual difference underlined above…

The injunction sought is to order Netlog to introduce, for all its customers, *in abstracto* and as a preventive measure, at its own cost and for an unlimited period, a system for filtering most of the information stored on its servers in order to identify files containing works in respect of which SABAM claims to hold rights, and to block the exchange of such files.

The injunction is claimed on the basis of article 8(3) of the InfoSoc Directive 2001/29/EC and article 11 of the Enforcement Directive 2004/48/EC, which provide the possibility of applying for an injunction against an intermediary whose services are being used by a third party to infringe IP rights. Both Directives provide however that they do not affect the provisions relating to liability (articles 12 to 15) in Directive 2000/31/EC. After noticing that the injunction sought would require the hosting service provider to carry out general monitoring, the CJEU concludes that it is prohibited by article 15(1) of the Directive 2000/31/EC.

Like in the Scarlet v. SABAM case, instead of limiting its reasoning to this mere application of the E-Commerce Directive, the CJEU further anchors its ruling on a balance to be stricken between several applicable fundamental rights. Citing case C-275 Promusicae, it repeats that the protection of intellectual property must be balanced against the protection of the fundamental rights of individuals which would be affected by the contemplated preventive measures.

According to the CJEU, the hosting service provider's freedom to conduct business would be impaired (article 16 of the Charter of Fundamental Rights of the European Union). The injunction would indeed require to install a complicated and costly, permanent computer system at its own expense, hurdling the provider to provide its services.

The CJEU also judges that users of the services would see their rights and freedoms undermined as well, as the filtering system would affect their right to privacy and the freedom to receive or impart information.