News about Internet Service Providers' Liability

The decision of the European Court of Justice on the case Sabam vs. Scarlet and the "Centemero" Draft Law currently under discussion at the Italian Parliament

Contents

1. The case Sabam vs. Scarlet

On November 24, 2011 (proc. no. C-70/10, Scarlet vs. Sabam), the European Court of Justice ("**ECJ**") ruled that the injunction, addressed by a national court to an Internet Service Provider (or "**ISP**"), to install a general filtering system (i.e. a filtering system intended for all users and for all electronic communications passing through the ISP's platform), as a preventive measure, exclusively at the ISP's expenses and for an unlimited period of time, for the purpose of blocking the transfer of contents infringing third party copyrights, conflicts with EU law.

By this decision the ECJ ruled on the preliminary question referred by the Court of Appeal of Brussels in the context of a litigation case arisen in Belgium between a Belgian ISP (Scarlet Extended SA, "**Scarlet**") and the local collecting society of authors, composers and editors of musical works (*Société Belge des Auteurs, Compositeurs et Editeurs SCRL*, "**Sabam**").

In 2004 Sabam, challenging that the users of Scarlet's services were used to download works belonging to Sabam's catalogue by means of "peer to peer" networks, without permission and without paying the relevant royalties, summoned Scarlet before the Tribunal of Brussels claiming the declaration of infringement of the copyright on the musical works contained in its catalogue, and the injunction to Scarlet to cease and desist from such infringement "by blocking, or making impossible for its customers, sending or receiving in any way files containing a musical work using peer-to-peer software without the permission of the relevant rightsholders" (see point 20 of the decision).

The President of the Tribunal of Brussels awarded the measures claimed by Sabam.

By appealing against such first instance judgment, Scarlet challenged the technical feasibility of the filtering and blocking systems enjoined by the Tribunal, and also claimed that such decision was contrary to EU legislation concerning (i) the Internet Service Providers' liability, since the filtering system at issue would entail for Scarlet a general obligation to monitor all communications on its network, and (ii) the personal data protection, since such filtering system would entail the disclosure of Scarlet users' IP addresses.

As a consequence, the Court of Appeal of Brussels suspended the appeal proceedings and referred to the ECJ the following preliminary question: whether EU law permits Member States to "authorize a national court […] to order an ISP to install, for all its customers, *in abstracto* and as a preventive measure, exclusively at the ISP's expenses and for an unlimited period of time, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software […]" in order to monitor the electronic files containing copyrighted works through its network (see point 28 of the decision).

By examining the above mentioned question, firstly the ECJ points out that the installation of the filtering system ordered by the first instance judge would oblige Scarlet to actively **monitor all data relating to all its customers in order to prevent any future infringement** of intellectual property rights, and specifies that such installation would entail, *de facto*, a **general monitoring activity** which is prohibited by art. 15(1) of the Directive 2000/31/EC on the electronic commerce.

The ECJ however does not declare only the inconsistency of such filtering systems with the Directive 2000/31/EC, but also points out that, even though art. 17(2) of the Charter of the Fundamental Rights of the European Union provides for the protection of the intellectual property right (protection enjoyed by copyright owners), such rights cannot be nevertheless regarded as "inviolable" rights, meaning that their protection must be balanced against the protection of other fundamental rights – e.g. the ISP's freedom to conduct a business – by the authorities and national courts.

In this regard, the most important principle stated by the ECJ on the case at stake appears to be that national court's injunctions imposing an ISP to install a general filtering system **would infringe the national courts' obligation to guarantee a fair balance** between, on the one hand, the intellectual property rights, and on the other hand:

1. the **freedom to conduct business**, since "*it would require Scarlet to install a complex, expensive, permanent computer system at its own expenses*" (see point 48 of the decision);
2. the **right of protection of the personal data** owned by Scarlet's customers as well as the **freedom to receive** or **impart information** (see point 50 of the decision);
3. the **freedom of information** since "*that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications*" (see point 52 of the decision).

Therefore, it is precisely on the basis of the above mentioned premises that the ECJ settled the preliminary question ruling that **the EU law precludes the injunction to an ISP to install a filtering system:** (i) **intended for all electronic communications passing via its services**, in particular those involving the use of "peer-to-peer" software; (ii) **which applies indiscriminately to all its customers;** (iii) **as a preventive measure;** (iv) **exclusively at its expenses;** and (v) **for an unlimited period** of time, for the purposes to identify, on the ISP's network, the electronic files containing copyrighted works in respect of which the applicant claims to hold intellectual property rights, and to block the transfer of such files.

2. The "Centemero" Draft Law

In the light of the above mentioned principles expressed by the ECJ, it is important to consider the Draft Law no. 4549 submitted to the Italian Parliament on July 26, 2011 by initiative of some deputies of the governing majority, and currently under discussion at the Italian Parliament (the "**Centemero Draft Law**"), with the aim of introducing new aspects of liability for the ISPs by integrating articles 16 and 17 of Legislative Decree no. 70 of April 9, 2003 (which implements in Italy the aforementioned Directive 2000/31/EC on the electronic commerce).

The Legislative Decree no. 70/2003, currently and *inter alia*, provides for: (i) the ISP's **obligation** to immediately activate itself in order to remove from its website the information which turned out to be unlawful or to disable access to such information **following a proper order by the competent authorities** (see art. 16), and (ii) the **lack** of any ISP's **general obligation to monitor** the information transmitted or stored on its platform, as well as the lack of any ISP's obligation **to actively seek** facts or circumstances showing the presence of unlawful activities on its platform (see art. 17).

For any further clarifications or research please contact:

Milan

Nino Di Bella
Tel. +39 02 763741
ndibella@gop.it

Luca Rinaldi
Tel. +39 02 763741
lrinaldi@gop.it

In this respect, the Centemero Draft Law – which consists of only two articles – would intervene, *inter alia*: (a) by integrating art. 16 of Legislative Decree no. 70/2003 so that the ISP would be bound to remove the unlawful information, or disable relevant access, **even following a proper notice "by any interested private party"** and not only by the competent authorities (see art. 1 of the Draft Law), without however providing for any *"*notice and take-down procedure*"*; and (b) by integrating art. 17 of Legislative Decree no. 70/2003 as follows: on the one hand, by keeping the provision stating the lack of a general ISP's monitoring obligation, but on the other hand by introducing (i) the **exclusion of the safe harbor** enjoyed by the ISPs pursuant to Legislative Decree no. 70/2003 **with respect to those ISPs which "provide also additional instruments or services, in particular organization or promotion services** […]", and (ii) a ***"*diligence duty"**, to be fulfilled by all ISP, aiming at **"indentifying and preventing certain types of unlawful activities"**, which should entail "inter alia: […] the use of **filtering systems**" which – ultimately – would prevent the transmission of contents infringing intellectual or industrial property rights "**prior to the on line entry**" of such contents (see art. 2 of the Draft Law).

In the light of the above mentioned principles stated by the ECJ in the Sabam vs. Scarlet case, it is worth therefore query whether the rules provided by the draft law no. 4549, currently under discussion at the Italian Parliament, and in particular (i) the exclusion of the safe harbor for all ISPs which provide also *"organization and promotion services"*, as well as (ii) the ISPs' obligation to install an apparently targeted *"filtering system"* ("apparently targeted" as aimed at identifying and preventing only "certain types*"* of unlawful activities, without however providing any details about the "types of unlawful activities" to "identify and prevent"), and basically preventive, with no time limit and exclusively at the ISP's expenses, comply with the EU law on the electronic commerce as interpreted by the ECJ; and to answer such question we also should assess whether the 5 conditions above mentioned which, for the ECJ, would make the injunction of filtering systems to ISPs contrary to EU legislation, are to be considered as "cumulative" or not.