**CJEU rules on standing of collecting societies and safe harbour availability**

*Coöperatieve Vereniging SNB-REACT U.A. v Deepak Mehta*, C-521/17, EU:C:2018:639

In its ruling in *SNB-REACT*, the Court of Justice of the European Union (CJEU) clarified at what conditions a collecting society has standing under Article 4(c) of Directive 2004/48 (the Enforcement Directive) and information society service providers (ISSPs) may rely on the safe harbours within Articles 12 to 14 of Directive 2000/31 (E-commerce Directive).

**Legal context and facts**

This referral from Estonia was made in the context of proceedings that a collecting society, SNB-REACT, had initiated against an individual, Deepak Mehta, concerning the latter's alleged liability for infringement of the intellectual property rights of ten trade mark owners. According to SNB-REACT, Mehta had allegedly registered a number of IP addresses and internet domain names, which unlawfully used signs identical to the trade marks owned by SNB-REACT members, together with websites unlawfully offering for sale goods bearing such signs. Mehta, however denied that he had registered the IP addresses and domain names challenged by the claimant. Even if he owned 38,000 IP addresses, he had rented them to third-party companies. Furthermore, this activity should be regarded as akin to that of a service providing access to an electronic communications network, together with an information transmission service, being – as a result – eligible for the safe harbour protection under the Estonian provisions corresponding to Article 12 to 14 of the E-Commerce Directive.

At first instance, SNB-REACT's action was dismissed on grounds that it would lack standing to bring legal proceedings in its own name to enforce its members' rights, also that Mehta was eligible, as an ISSP, for the safe harbour protection.

SNB-REACT appealed to the Tallinn Court of Appeal, which made a reference to the CJEU and asked:

(1) Is Article 4(c) of [the Enforcement Directive] to be interpreted as meaning that Member States are required to recognise bodies collectively representing trade mark proprietors as persons with standing to pursue legal remedies in their own name to defend the rights of trade mark proprietors and to bring actions before the courts in their own name to enforce the rights of trade mark proprietors?   
(2) Are Articles 12, 13 and 14 of [the E-commerce Directive] to be interpreted as meaning that even a service provider whose service consists in registering IP addresses, thus enabling them to be anonymously linked to domains, and in renting out those IP addresses, is to be regarded as a service provider within the meaning of those provisions to whom the exemptions from liability provided for in those articles apply?

**Analysis**

The CJEU answered both questions in the affirmative, without seeking the prior Opinion of the appointed Advocate General (Wathelet).

***Standing of collecting societies***

Article 4(c) of the Enforcement Directive provides that intellectual property collective rights management bodies, which are regularly recognized as having a right to represent holders of intellectual property rights, in so far as permitted by and in accordance with the provisions of the applicable law, are entitled to seek application of the measures, procedures and remedies referred to in that piece of legislation.

The CJEU deemed it necessary to clarify the meaning of ‘applicable law’ and ‘as permitted’ in that provision. First, the expression 'applicable law' refers to both EU and national laws, as appropriate. Second, Member States do not enjoy unlimited discretion as to whether or not recognize collecting societies as having standing. Third, as is apparent from Recital 18 in the preamble to the Enforcement Directive, EU law intended to grant standing also to those having a direct interest in the defence of third-party rights.

It follows that, where a collecting society is regarded by national law as having a direct interest in the defence of its members' rights and that law allows that body to bring legal proceedings, the Member States are required to recognize such collecting society as a person entitled to seek application of the measures, procedures and remedies provided for by the Enforcement Directive, and to bring legal proceedings for the purpose of enforcing such rights.

***Liability of providers of IP address rental and registration service***

Turning to the second question, the CJEU reviewed the conditions at which the safe harbours within Article 12 to 14 of the E-commerce Directive apply. First, the Court tackled the question whether the provider of an IP address rental and registration service (as was the defendant in the background proceedings) could be deemed an ISSP for the sake of the E-commerce Directive. The Court noted how this notion is fairly loose, in that the concept of ‘information society service’ refers to services which are provided: at a distance; by means of electronic equipment for the processing and storage of data; at the individual request of a recipient of services; normally in return for remuneration. It is a notion that includes services contributing to facilitating relations between persons engaged in online sales activities and their customers. The CJEU found that it did not have sufficient evidence to determine whether a service like that one at issue in the background proceedings would fall within the notion of information society service, but it did not exclude it.

Then the CJEU turned to consideration of the conditions at which the 'limitations of liability', that is the safe harbours under the E-commerce Directive, apply. To make such determination it is necessary, first, to identify whether the information society service at issue consists of mere conduit (Article 12), caching (Article 13) or hosting (Article 14) and, then, review whether the conditions for the safe harbour for the specific service at issue are satisfied. For all three scenarios, the safe harbour only applies where the activity of the information society service provider is of a mere technical, automatic, and passive nature. This implies that that service provider has neither knowledge of nor control over the information which is transmitted or stored by the persons to whom he provides his services. By contrast, the safe harbours are unavailable in the case where an ISSP plays an active role, by allowing its customers to optimise their online sales activity (para 48). Having said so, the CJEU stated (para 50):

it is for the referring court to satisfy itself, in the light of all relevant facts and evidence, as to whether such a service provider has neither the knowledge of nor control over the information transmitted or cached by his clients and whether he does not play an active role by allowing them to optimise their online sales activity.

**Practical significance**

The most relevant aspect of the decision relates to the Court’ analysis of safe harbour availability. In particular, the reasoning at paragraphs 48 to 50 appears construed in light of landmark safe harbours decisions like *Google France SARL and Google Inc. v Louis Vuitton Malletier SA* (C-236/08), *Google France SARL v Viaticum SA and Luteciel SARL* (C-237/08) and *Google France SARL v Centre national de recherche en relations humaines (CNRRH) SARL and Others* (C-238/08), EU:C:2010:159 (*Google France*) and *L’Oréal SA and Others v eBay International AG and Others*, C-324/09, EU:C:2011:474 (*L’Oréal*), yet the wording is not identical. In those cases the CJEU linked the active role of the provider which excludes the availability of the safe harbour to knowledge of or control over of third-party information. In *Google France* the Court held (para 120):

Article 14 of Directive 2000/31 must be interpreted as meaning that the rule laid down therein applies to an internet referencing service provider in the case where that service provider has not played an active role of such a kind as to give it knowledge of, or control over, the data stored. If it has not played such a role, that service provider cannot be held liable for the data which it has stored at the request of an advertiser, unless, having obtained knowledge of the unlawful nature of those data or of that advertiser’s activities, it failed to act expeditiously to remove or to disable access to the data concerned.

Similarly in *L'Oréal* the Court stated (para 113):

Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.

In those cases the logic was the following:   
  
active role → knowledge of or control over information → unavailability of safe harbours  
  
While in *SNB-REACT* the process is different (see also para 52)

knowledge of or control over information + active role (eg optimization of online sales activities) = unavailability of safe harbours

As it appears to be the case when the Court decides without the prior Opinion of the appointed AG, the resulting reasoning is not as straightforward as one would wish. The approach to the definition of the conditions for excluding the availability of the safe harbours is telling: are paragraphs 50 and 52 in the judgment just the result of rather imprecise writing or has the Court, instead, inaugurated a new approach to the definition of the conditions for the E-commerce safe harbours? That remains to be seen.

Eleonora Rosati

JIPLP and University of Southampton

eleonora@e-lawnora.com