IIC
DOI 10.1007/s40319-014-0292-x

ARTICLE

Much Ado about Little – Privately Litigated Internet Disconnection Injunctions

Martin Husovec · Miquel Peguera

Abstract In this article we examine the legal framework of the European Union for injunctions against intermediaries whose services are used by a third party to infringe an intellectual property right, as set forth in the InfoSoc Directive and the Enforcement Directive. In particular, we consider the conditions to apply for the injunctions, taking into account how those conditions have been construed by the CJEU. We explore which is the minimum floor of injunctive relief Member States are obliged to provide under the Directives, as well as the maximum ceiling allowed, beyond which the protection granted would infringe upon the limits imposed by EU law. Next, we move on to consider particular types of injunctions that right holders may apply for against intermediaries on the basis of Art. 8(3) of the InfoSoc Directive, namely those that would consist of enjoining an ISP from providing Internet access to one of its users allegedly engaging in copyright infringement. A case already decided in Spain, *Promusicae et al. v. R Cable y Telecomunicaciones Galicia*, granting such an injunction serves us as a study case to assess the problems these remedies face. On the one hand, these privately litigated Internet disconnection injunctions may be seen by right holders as a promising tool to fight online copyright infringement – perhaps an alternative to unsuccessful graduate response schemes. However, as we show in this article, these injunctions raise serious issues regarding their compatibility with the EU Charter of

The authors would like to thank Professor Annette Kur, Cédric Manara, Ellen Wesselingh, Pekka Savola and the IIC peer reviewer for their inspiring comments on an earlier draft.

M. Husovec (✉)
IMPRS-CI Doctoral Research Fellow
Max Planck Institute for Innovation and Competition, Munich, Germany
e-mail: martin@husovec.eu

M. Peguera
Associated Professor of Law
Universitat Oberta de Catalunya, Barcelona, Spain
e-mail: mpeguera@uoc.edu

Published online: 03 February 2015

Fundamental Rights. Indeed, the possibility of effective injunctions of this kind which conform with human rights turns out to be very narrow. In other words, the Directive's provisions promise much, but if applied correctly, they deliver little.

Keywords ISP liability · Injunctions against intermediaries · Secondary liability · Internet disconnection injunctions · Graduated response · Three strikes

Introduction

Copyright and related right holders tend to look at Internet service providers (ISPs) as essential actors in their fight against online copyright infringement. In particular, right holders have sought the cooperation of ISPs to curb illegal file sharing, trying to get them involved in different types of so-called graduated response schemes, which have been adopted in a number of countries in recent years.[1] Unrelated to the graduate response systems, European Union (EU) law already provides a way for right holders to obtain some compulsory cooperation from ISPs. In particular, Art. 8(3) of the InfoSoc Directive[2] sets forth that Member States must allow right holders to apply for an injunction against intermediaries – including ISPs – whose services are used by a third party to infringe their rights. Under the national implementations of this provision, different courts have issued blocking injunctions against ISPs so that they prevent their users from accessing a particular website.[3] However, in a recent case, a Spanish court of appeal has also accepted the national transposition of Art. 8(3) as a valid ground to order an ISP to cease providing Internet access to one of its subscribers allegedly engaging in P2P file sharing. While applying for this sort of Internet disconnection injunction might end up being a new trend in the fight copyright infringement, it is submitted that such an injunction is hardly consistent with human rights limits, such as the right of fair trial, the required "quality of the law", and the principle of proportionality. There is a huge gap between what the provision seems to allow and what is actually permissible.

Part 1 of this article discusses the EU legal framework regarding injunctions against innocent intermediaries, showing its potential and limits. Part 2 presents the Spanish case *Promusicae v. R* as a study case of a disconnection injunction under a national law implementing the InfoSoc Directive. Part 3 analyzes the implications and limits of such an injunction, focusing particularly on the right to fair trial, the quality of the law, and the principle of proportionality. Part 4 offers a brief conclusion.

[1] Legislation implementing graduated response schemes has been adopted in France, the UK, New Zealand, Taiwan and South Korea. In addition, private agreements between right holders and ISPs have been reached in a number of countries, including Ireland and the US. *See* Giblin (2014), Bridy (2012), Yu (2010).

[2] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (hereinafter "InfoSoc Directive").

[3] *See*, *e.g. UPC Telekabel Wien* C-314/12.

1 European Union Law

European intellectual property law generally does not explicitly address secondary liability for intellectual property violations – the tort liability of someone other than the direct infringer.[4] The only exceptions are the anti-circumvention provisions of the Software and InfoSoc Directive[5] and the Agreement on the Unified Patent Court (AUPC).[6] There is some debate over whether some of the secondary legislation does implicitly also cover secondary liability,[7] but so far, such a question has never been articulated and subsequently answered in a clear manner.[8] On the other hand, EU law establishes liability exclusions through the E-Commerce Directive's safe harbors[9] – which in turn set out some limits on the Member States' discretion for imposing liability on intermediaries.

While failing to address secondary liability, or perhaps to overcome this failure, EU law does legislate certain availability of injunctions against those who do not directly infringe[10] the intellectual property rights, regardless of whether or not they may be considered secondarily liable under the applicable national law. These rules are included in Art. 8(3) InfoSoc Directive (for copyright and related rights), Art. 11 of the Enforcement Directive[11] (for other intellectual property rights) and Art. 63(1) AUPC (for the Unitary patent). All of these provisions use basically identical wording requiring that Member States ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right.

The framework of this remedy against intermediaries is potentially endlessly broad, with very far-reaching consequences for society. The EU's secondary legislation and CJEU's interpretation of it present only very few obstacles for

[4] *See* Leistner (2014), Husovec (2013); Max Planck Institute for Intellectual Property & Competition Law Research Paper No. 13–14.

[5] *See* Leistner (2014), p. 75.

[6] Article 26 AUPC provides: "(1) A patent shall confer on its proprietor the right to prevent any third party not having the proprietor's consent from supplying or offering to supply, within the territory of the Contracting Member States in which that patent has effect, any person other than a party entitled to exploit the patented invention, with means, relating to an essential element of that invention, for putting it into effect therein, when the third party knows, or should have known, that those means are suitable and intended for putting that invention into effect".

[7] *See* Husovec (2013), p. 117.

[8] *See* Husovec (2013), footnote 5, reporting about the *Donner* case, C-5/11, where the CJEU read into the autonomous notion of the "distribution right" arguably also the test for secondary infringements in para. 27 of the decision, and *L'Oreal SA & Ors v. eBay International AG & Ors* [2009] EWHC 1094 (Ch), where Justice Arnold considers the possibility of Union secondary liability.

[9] Articles 12–15 of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (hereinafter "E-Commerce Directive").

[10] The recent case of *UPC Telekabel Wien* C-314/12 refers to an Internet access provider as someone who "is not the author of the infringement of the fundamental right of intellectual property which has led to the adoption of the injunction" (*UPC Telekabel Wien*, para. 53). *See* more discussion in Husovec (2014).

[11] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (hereinafter "Enforcement Directive").

plaintiffs seeking to take advantage of it. Not only are the prerequisites of the remedy very loose, but also the limitations are very vague and displaying little sophistication – mostly relying on the general human rights framework. In this Part 1 we will try to unpack several of the most important issues related to both the capacity of the remedy and its various limitations, before we proceed with the analysis of the study case in the subsequent sections.

1.1 Scope of the Injunctions against Intermediaries

In order to establish a course of action, the plaintiff has to prove following elements: (a) the defendant is an "intermediary", (b) "whose service are used", (c) "by a third party", (d) "to infringe". In practice, none of these conditions present a real hurdle for the plaintiff. It needs to be pointed out, however, that neither Art. 8(3) InfoSoc Directive nor Art. 11 of the Enforcement Directive harmonize the exact conditions triggering such injunctions,[12] which are left to the national laws of the Member States.[13] Thus the Member States are free to implement the provisions not only verbatim, but also with additions, provided that they satisfy the minimum binding floor of protection to which we refer below.

First, (a) the term "intermediary" in the sense of Art. 8(3) InfoSoc Directive and Art. 11 Enforcement Directive is interpreted by CJEU case law in a broad manner, including basically anyone who "provide[s] a service *capable of being used* by a third party to infringe".[14] Thus Internet access providers, as well as providers of payment or anonymizing services, may all be covered by the definition in most circumstances – and so might be various off-line intermediaries. Even an intermediary such as an electricity provider or a bank cannot be ruled out.[15] Second, as the currently accepted website blocking injunctions show, there is not even a need for an alleged infringer who (b) uses the service to infringe to be a customer of the concerned intermediary.[16] It suffices that the services are capable of serving as a communication channel for the infringements.[17] No affiliation is required. The term is thus perceived teleologically beyond its natural meaning in the language.[18] The only criterion and limit seems to be the ability of an online *or* off-line service provider to put an end to an infringement.[19]

[12] *See* Recital 23 of the InfoSoc Directive; Recital 59 of the Enforcement Directive. *See also Scarlet Extended* C-70/10, para. 32 and *Netlog* C-360/10, para. 30.

[13] Article 63(1) AUPC appears to be an autonomous rule with its own preconditions.

[14] *See* CJEU, *Tele 2*, C-557/07 (emphasis added).

[15] However unlikely, an electricity provider, for instance, could be theoretically sued as an off-line intermediary to cut off the access to electricity to an infringing factory. Application of these injunctions to off-line intermediaries have arrived before the CJEU so far only once in *Frisdranken*, C-119/10 in the context of the Advocate General's opinion.

[16] *See UPC Telekabel Wien*, C-314/12, para. 34.

[17] *Ibid.*

[18] Angelopolous (2009) CJEU in UPC Telekabel Wien: A totally legal court order … to do the impossible. Kluwer Copyright Blog. Available at http://kluwercopyrightblog.com/2014/04/03/upc-telekabel-wien/.

[19] Compare this rationale with "in rem injunctions" in the civil law countries – *see* Husovec (2013).

Third, (c) the person using the services to infringe can be either a primary or a secondary infringer. Although the CJEU has not confirm this explicitly, UK courts have had so far very little difficulty in accepting this.[20] Lastly, (d) one would expect that at least the present tense in the language of the provision – "services [which] *are used* by a third party to infringe" – could limit the reach of injunctions to actually committed infringements, excluding those not yet started. This is, however, an open issue. It is the question of whether these injunctions against intermediaries are also available in the form of preemptive relief,[21] i.e. in the form of an injunction to restrain wrongful acts which are threatened or imminent but have not yet commenced. The question is whether Art. 8(3) InfoSoc and Art. 11 of the Enforcement Directive require that at least an infringement by a user has already been committed, or to the contrary, the mere danger of a potential infringement by a user would suffice. The wording of both provisions – "intermediaries whose services *are used*" – would suggest that preemptive injunctions are not prescribed. A similar reading seems to result from Recital 59 InfoSoc Directive, which states that "[i]n many cases such intermediaries are best placed to bring such infringing activities *to an end*." The CJEU, however, challenged this reading in *L'Oreal v. eBay,* C-324/09 when it ascribed also a preventive function to these kinds of injunctions.[22] It did so relying on Recital 24 in the preamble to the Enforcement Directive, which declares that, depending on the particular case, and if justified by the circumstances, measures aimed at preventing further infringements of intellectual property rights must be provided for. From this background, it would not come as a surprise if this preventive function would extend not only to the future curbing of already committed infringements, but also to preventing threatened and not yet materialized infringements of users.[23] It must be reminded, however, that depending

[20] If the person who uses the services of an Internet access provider is not a user, but a targeted website in the website blocking cases, the infringing acts often rely on the secondary liability of those websites. This is most likely the case even in the situation that gave rise to the *UPC Telekabel Wien* reference, but also in other national cases in the UK, such as *Newbiz II* [2011] EWHC 1981 (Ch) (the website operator is secondary liable for joint tortfeasorship and authorization of an infringement); *Newbiz II* [2011] EWHC 2714 (Ch); *Dramatico* [2012] EWHC 268 (Ch) (paras. 81, 83 – the website operator is secondary liable for joint tortfeasorship and authorization of an infringement); *Dramatico* [2012] EWHC 1152; *EMI Records* [2013] EWHC 379 (Ch) (paras. 70, 74 – the website operator is secondary liable for joint tortfeasorship and authorization of an infringement); *FAPL v. Sky* [2013] EWHC 2058 (Ch) (para. 43 – alternatively is the website operator also secondary liable for joint tortfeasorship); *Paramount v. Sky* [2013] EWHC 3479 (Ch) (para. 35 – alternatively is the website operator also secondary liable for joint tortfeasorship).

[21] In common law also called *quia timet* injunctions.

[22] Both the InfoSoc and Enforcement Directives require that the measures which the Member States must take in order to conform to those directives are aimed not only at bringing to an end infringements of copyright and related rights, but also at preventing them (*see* to that effect for the InfoSoc Directive: *Scarlet Extended*, C-70/10, para. 31; *Netlog*, C–360/10, para. 29; *UPC Telekabel Wien*, C-314/12, para. 37; and for the Enforcement Directive: *L'Oreal v. eBay*, C-324/09, para. 144).

[23] Germany accepted this in the famous decision of the Federal Supreme Court, *Internetversteigerung II.*, I ZR 35/04. The most recent decision by the CJEU in *UPC Telekabel Wien* suggests however the unavailability of such injunctions: "in order to obtain the issue of an injunction against an internet service provider, the holders of a copyright or of a related right *must show that some of the customers of that provider actually access, on the website at issue, the protected subject-matter made available to the public without the agreement of the rightholders*" (*UPC Telekabel Wien*, para. 36).

on the preconditions in the national law,[24] such an effect could be at least temporarily achieved also by preliminary injunctions.

A possible limitation for extending the injunction to all ISPs in a country might arise, however, from the argument that the ISPs which do not supply Internet access to the alleged infringer are not "intermediaries whose service are being used" to infringe. Nonetheless, this might depend on the nature of the alleged infringing acts. If the person concerned were allegedly engaging in file sharing, then all the other access providers could arguably be seen as channels through which that user delivers the infringing content to those ISPs' customers. If however, the activity concerned were illegal downloading from cyber-lockers[25] or accessing unauthorized web streaming,[26] then nothing is communicated to the users of other access providers, and hence their services could not be seen as being "used by third party to infringe". Even this could be overcome if the CJEU were to accept the above analyzed possibility of preemptive injunctions, i.e. injunctions against intermediaries whose services are *not yet* used by the said user to infringe, but where there is an imminent danger that they will if those ISPs are not precluded from entering into a contract with that user.

Finally, it must be noted that the safe harbors laid down in the E-Commerce Directive, while protecting intermediaries from liability, do not limit the possibility of injunctive relief or claims for information available under the national law. All the safe harbors, including the one that covers mere conduit services such as those provided by Internet access providers (Art. 12 E-Commerce Directive), unambiguously permit injunctions to be granted. This is confirmed not only by the cases of *Sabam* and *Scarlet Extended* and by the scholarly literature,[27] but mainly by the *UPC Telekabel Wien* case. There the CJEU allowed, as compatible with the maximal admissible ceiling under some circumstances,[28] website blocking injunctions issued against non-liable access providers. Thus it implicitly confirmed what the Advocate General had explicitly formulated as follows:

[24] The national law is subject to Art. 9(1) of the Enforcement Directive, which states "Member States shall ensure that the judicial authorities may, at the request of the applicant: (a) issue against the alleged infringer an interlocutory injunction …; an interlocutory injunction may also be issued, under the same conditions, against an intermediary whose services are being used by a third party to infringe an intellectual property right; injunctions against intermediaries whose services are used by a third party to infringe a copyright or a related right are covered by Directive 2001/29/EC".

[25] The CJEU recently decided in *ACI Adam* C-435/12 that downloading from illegal sources does not qualify for the private copying exception. Surprisingly, this conclusion came not as a result of the three-step test considerations, but directly as an interpretation of Art. 5(2)(b) of the InfoSoc Directive.

[26] CJEU, *Public Relations Consultants Association*, C-360/13 (holding that even transient copies under Art. 5(1) InfoSoc are subject to the three-step test of Art. 5(5)). In German, Hannover District Court, Judgment 550 C 13749/13, 27 May 2014 (coming to conclusion that web-streaming from *illegal sources* can constitute an infringement).

[27] Angelopolous (2009); Meale (2011); Peguera (2010), paras. 24, 61–62; Koziol (2012); Halldórsdóttir (2004); Jakobsen (2011a, b) and Czychowski and Nordemann (2013) ("*Die Privilegierung gilt nur für Schadensersatzansprüche (und damit zusammenhängende Ansprüche wie sie vorbereitende Auskunftsansprüche) und für bußgeld- sowie strafrechtliche Sanktionen, aber nicht für Unterlassungsansprüche*").

[28] *See more* in Husovec (2014) p. 2.

> The liability rules for intermediaries, which are laid down in Directive 2001/31, *do not, in principle, preclude the issuing of an injunction* under Article 8(3) of Directive 2001/29 against ISPs. It is true that Article 12 of that directive contains special rules on the liability of intermediary service providers as mere conduits of information. However, under paragraph 3 of that provision, those rules do not affect the possibility for a court or administrative authority of requiring the service provider to terminate or prevent an infringement.[29]

1.2 Binding Minimum Floor of Injunctive Relief

As mentioned earlier, the European legislator left it to the Member States to provide for the whole set of requirements for the injunctions against intermediaries in Art. 8(3) InfoSoc Directive and Art. 11 Enforcement Directive. This, however, did not stop the CJEU from requiring a certain minimum floor of injunctive relief, which must be provided in any event. This binding minimum was derived from the doctrine of *effet utile*,[30] according to which, amongst several possible interpretations, the one that best guarantees the practical effect of Union law must prevail. Based on this principle, in *L'Oreal v. eBay* the CJEU postulated that the rules of national law must "be designed in such a way that the objective pursued by the directive may be achieved".[31] Otherwise, the minimum floor of protection afforded by Union law would be breached because a Member State would fail to comply with its obligation to provide for meaningful injunctions of this kind. It is for those reasons that the measures concerned must be at least "effective and dissuasive".[32] In other words, if the injunctive relief available against intermediaries is not effective and dissuasive enough, the national law is incompatible with Art. 8(3) InfoSoc Directive and Art. 11 Enforcement Directive.

Therefore, the question arises as to exactly how far the preconditions of national law may extend, and particularly whether or not national law may establish the prerequisite that the intermediary must be directly or secondarily liable for the injunction to be granted. From a systematic point of view, both Art. 8(3) InfoSoc Directive and Art. 11, third sentence, of the Enforcement Directive deal with injunctions against intermediaries *after* remedies against infringers. In the InfoSoc Directive, injunctions against intermediaries appear after Art. 8(1), which deals with "sanctions and remedies in respect of infringements of the rights and obligations". In the Enforcement Directive, they appear after the first sentence of Art. 11 referring to the power of "the judicial authorities [to] issue against the infringer an injunction". This begs the following question: do these preceding provisions refer only to harmonized, direct, or also to non-harmonized, secondary (indirect) infringers? And are Art. 8(1) with Art. 8(3) InfoSoc Directive, and Art. 11 first

[29] Opinion of Advocat General Cruz Villalón, 26 November 2013, Case C-314/12, *UPC Telekabel Wien*, para. 52 (emphasis added).

[30] Mayr (2013).

[31] *See L'Oréal v. eBay*, para. 136.

[32] *Ibid.*

sentence of the Enforcement Directive with Art. 11 third sentence, mutually exclusive provisions? Or do they overlap when an intermediary is an infringer itself? This is a very complex question, which exceeds aims of this article.[33]

Arguably, if a national law would require a showing of secondary liability in order to grant the injunction, it could in some cases go against the purposes of the InfoSoc Directive as it would restrict the availability of the injunctions too much. This would especially be the case due to the fact that intermediaries are generally exempted from secondary liability under Art. 12 of the E-Commerce Directive.[34] For intermediaries not covered by the safe harbours and only subject to national secondary liability doctrines, such as payment intermediaries, the possibility of conflict would depend on how easily those doctrines establish liability. After all, it cannot be completely ruled out that national secondary liability doctrines unrestricted by the Union law could reach the point of holding those intermediaries liable.

1.3 Human Rights Limits as (the only) Binding Ceiling?

Although preconditions of injunctions can differ from Member State to Member State, they all are subject to a common maximal admissible ceiling beyond which such injunctions may not be provided, as they would go against EU Law. This binding ceiling is embodied in the overarching principles of proportionality and reasonableness of the requested measures.[35] The more detailed criteria listed in Art. 3 of the Enforcement Directive, demanding that measures be fair, uncomplicated, cheap, non-abusive, and do not create barriers to legitimate trade, can be seen as a mere specification of these overarching principles.[36] The same can be said of the requirements established by the CJEU in the context of open-ended website blocking, such as those of *locus standi* for users and transparency of the injunctions.[37]

Despite the strong human rights connotations of these criteria, it would be probably mistaken to think that all of them embody only value judgments made within the framework of the EU Charter of Fundamental Rights (Charter). But this is nonetheless far from clear. It is true that many of the cases where the measures were deemed to go beyond the admissible ceiling are based on principles of the Charter applied to the rules on injunctive relief.[38] However, the fact that the cases

[33] The research of one of the authors (Martin Husovec) explores this interrelation in a greater detail – *See* the project website www.accountablenotliable.org.

[34] In spite of this, some Member States' transpositions appear to require secondary liability on the part of the intermediary. *See* Jakobsen (2011a).

[35] *See* a simplified version of Art. 3 of the Enforcement Directive criteria in Art. 42 of the Agreement on Unified Patent Court.

[36] For a more detailed argument of this kind *see* European Information Society Institute. "EISi Intervenes in Delfi AS v. Estonia before the ECHR", Available at: http://eisionline.org/index.php/projekty-m/sudy-a-obcianska-spolocnost-m/77-delfi-echr.

[37] *See more* in Husovec (2014), pp. 3–4;.

[38] In some countries general clauses like these are used to implement human rights considerations (indirect effect) in the ordinary law; *see more* Seifert (2011).

handed so far, such as *Scarlet Extended* C-70/10, *Netlog* C-360/10 and *UPC Telekabel Wien* C-314/12, had strong fundamental rights dimensions, and were rejected probably also as "Charter matters", does not mean that all of the upcoming cases will always need to acquire this intensity of a social problem in order to be rejected. For instance, it should also be possible to reject as inadmissible certain injunctions that are perfectly conform with all the human rights concerned but very ineffective. Proportionate, but ineffective (useless) measures should be prevented as matter of ordinary law – secondary legislation. Only in this way, the socially wasteful enforcement practices can be outright prevented.[39] Effectiveness should thus preserve a meaning autonomous to the proportionality test. The current tendency of the CJEU seems to be, however, different. It is a tendency to solve many issues not as a matter of secondary legislation, but as human rights issue.[40]

Because any injunction provided against intermediaries is ultimately an implementation of European Union law, all possible conflicts with fundamental rights and freedoms will also always need to be tested against the provisions of the Charter (see Art. 51(1)[41]), and not merely against the national constitutions. The Charter as a source of law will therefore strongly guide many Member States' courts in their application of various injunctions against intermediaries. Possible differing levels of protection of fundamental rights at the national and European level will sometimes need to be adjusted to the "Charter standards", regardless of whether they must be lowered or increased for these purposes.[42] This for instance means that should the national court seek to reject an injunction against an intermediary under considerations of a right to a fair trial of an unrepresented user, it could be required to explore the compatibility of such decision with the Charter provision (here Art. 47), perhaps even by means of a reference for a preliminary ruling to the CJEU.[43] Such a reference could then prevent a possible incompatibility with national human rights considerations, which bar such injunctions but are not shared by the CJEU, who is interpreting the respective provision of the Charter. In these cases, the

[39] The Hague Court of Appeal was reported to lift the website blocking injunction of "*ThePirateBay*" against Ziggo and XS4All due to considerations of ineffectiveness quoted in a qualitative study conducted by IViR; *see* http://www.worldipreview.com/news/dutch-court-lifts-pirate-bay-blocks.

[40] *See more* in Husovec (2014), p. 2.

[41] *See* CJEU, *Åklagaren*, C-617/10.

[42] In the *Melloni* case, C-399/11, the CJEU postulated that Art. 53 of the Charter "confirms that, where an EU legal act calls for national implementing measures, national authorities and courts remain free to apply national standards of protection of fundamental rights, *provided that the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of EU law are not thereby compromised*". An example of the need to lower the standards due to need to preserve "primacy, unity and effectiveness of the EU law" may be found in the decision of the Spanish Constitutional Court that followed the *Melloni* case, Case No. STC 26/2014. (*See* more at: http://europeanlawblog.eu/?p=2261#sthash.PqfRLuAC.dpuf). The Spanish Constitutional Court had to lower its domestic right to fair trail standards. For more on impact of *Melloni* decision *see* Weiß (2013); JHR and LB (2013). Moreover, in an increasing number of countries, the Charter itself is becoming a benchmark next to national constitutions; *see* Grabenwarter and Vranes (2013) and there cited decision of the Austrian Supreme Court (VfGH, U 466/11-18, paras. 35, 38).

[43] A similar situation arises in the context of the right to information and its conflict with the data protection framework; *see* the CJEU cases *Promusicae* C-275/06, *Tele 2* C-557/07, and *Bonnier Audio* C-461/10.

national court could be forced by EU law to provide for an injunction against an intermediary despite its national human rights doubts, but only if it can be said that such injunctions are required as a minimum protection under either Art. 8(3) InfoSoc Directive or Art. 11 Enforcement Directive.

To complicate things more, also the European Court of Human Rights (ECtHR) may become involved. If a provider or a user is dissatisfied with a national outcome even after the preliminary reference scrutiny before the CJEU, they might seek redress before the ECtHR, which could potentially view the interpretation of the Charter by the CJEU as insufficient to comply with the European Convention on Human Rights (Convention). In such a case, an open conflict between the CJEU and ECtHR could arise, and would need to be resolved probably as a subsequent reference for a preliminary ruling to the CJEU.[44] This conflict is not merely theoretical. If, for instance, UPC were obliged to open-ended website blocking injunctions by the Austrian courts after the reference of *UPC Telekabel Wien* comes to back to the national court, UPC could still seek a redress before the ECtHR by means of a complaint.[45]

Application of human rights as limits to privately litigated injunctions also pose more fundamental questions: namely, the extent and manner to which the Charter can oblige and shape capabilities of private parties among themselves (horizontal effect of human rights). Because ISPs are often private individuals without any ties with the state powers, as are the copyright holders, the question is when (if at all) and how much should human rights prerogatives also limit actions of individuals – and not only those of the state. Although the idea of horizontal effect of human rights is not new to the courts of most European countries, including the ECtHR,[46] the struggle of the CJEU case law to moderate private intellectual property disputes via human rights law will be very exciting to watch. The evidence that we might witness a more tectonic shift is well demonstrated in the recent *UPC Telekabel Wien*, where the CJEU required:

> [If] *the internet service provider adopts* measures which enable it to achieve the required [abstract] prohibition, the national courts will not be able to carry out such a review [that the measures do not affect internet users who are using the provider's services in order to lawfully access information] at the stage of the enforcement proceedings if there is no challenge in that regard. Accordingly, in order *to prevent the fundamental rights* recognised by EU law *from precluding the adoption of an injunction* such as that at issue in the

[44] The ECtHR and CJEU usually reflect on each other's positions. An example can be find in the case of *N. S.* C-411/10 and *M. E.* C-493/10, which followed *after* the decision of the ECtHR in *M.S.S. v. Belgium and Greece*, App. No. 30696/09, which found that, when applying the Dublin II Regulation, the Belgian Kingdom infringed Art. 3 of the ECtHR by exposing the asylum applicant to the risks linked to the deficiencies in the asylum procedure in Greece and to detention and living conditions in Greece. The CJEU subsequently adopted the view of the ECtHR and made the procedure under Dublin II Regulation more sensitive to rights of asylum seekers adjusting it by means of the EU Charter; *see more* in Laffranque (2012).

[45] For the argument of incompatibility of open-ended website blocking with the Convention, *see* Husovec (2014).

[46] *See* Seifert (2011), at 696.

main proceedings, *the national procedural rules must provide a possibility for internet users to assert their rights before the court once the implementing measures taken by the internet service provider are known*.[47]

This requirement of *locus standi* for users arguably violates the basic principle of the ECtHR case law. Namely, that any horizontal effect of freedom of expression based on doctrine of "positive obligations" can prescribe the state only to act to achieve a certain situation among individuals in conformation with human rights, and not to act in a form of a specific measure.[48] And further that individuals cannot directly invoke their human rights prerogatives against other individuals, but still only against the state.[49] The Austrian Supreme Court applying the CJEU's *ratio decidendi* above in the follow-up proceedings showed readiness not only to provide for such a horizontal effect indirectly, by basing it in the contractual arrangement between the ISP and its customer, but also directly by safeguarding it, if needed, by an action in law of torts.[50] The latter could be revolutionary especially if applied also in the context of voluntary disconnection schemes, where the state powers (courts) are not even remotely involved.

1.4 Sanction or Cooperation?

For the purposes of this article, we can conclude at least that a requirement of "effective and dissuasive" measures is probably more result-oriented than doctrinally-oriented; pointing to the economic principle of the cheapest-cost avoider,[51] rather than to national legal classifications. Nonetheless, from the standpoint of national legal categories, and with a long-term perspective, given the different forms in which these injunctive measures come today, many of them will be increasingly difficult to understand with the tort law mindset of sanctions.[52] In most cases, they could be best described as some type of "obligatory cooperation remedies" against intermediaries in the same way as they today understand various injunctions for disclosure of identity of users.[53] The need for this view is reinforced by the European Commission itself, which in its official report on the application of the Enforcement Directive[54] states: "Injunctions against intermediaries are *not intended as a penalty* against them, but are simply based on the fact that such

[47] *See* Telekabel, C-314/12 para. 57 (emphasis added).

[48] *See* Seifert (2011), 698.

[49] *See* Seifert (2011), 698.

[50] *UPC Telekabel Wien*, Austrian Supreme Court (OGH), Judgment 4 Ob 71/14 s, 24 June 2014.

[51] *See also* discussion in Dinwoodie (2014); and more generally Gilles (1992).

[52] This point is already made in Husovec (2013), p. 118 *et seq.*

[53] *See* Art. 8 of the Enforcement Directive.

[54] Commission Staff Working Document: Analysis of the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights in the Member States – accompanying document to the Report from the Commission to the Council, the European Parliament and the European Social Committee on the application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights COM(2010) 779 final.

intermediaries (e.g. Internet service providers) are in certain cases in the best position to stop or to prevent an infringement."

Putting doctrinal issues aside, when examining the practical reach of these injunctions, in cases such as *Scarlet Extended* or *UPC Telekabel Wien*, it becomes clear that they extend beyond most of the situations where national laws would find secondary liability.[55] Indeed few countries would be ready to regard ordinary Internet access providers as secondary infringers, thus attributing them the conduct of their users in a full range – leaving aside the fact that they will be normally covered by the Art. 12 of E-Commerce Directive anyway.

This paper builds upon the idea of injunctions against intermediaries as "cooperative remedies"[56] and examines one of their forms that might soon become a trend around European jurisdictions, similarly as website blocking injunctions began to be some time ago.[57] The privately litigated disconnections from Internet access are in a sense only a continuation of the increasing attempts to engage intermediaries in copyright enforcement. Their logic is that an Internet access provider, regardless of its own eventual liability, is in a position to assist a right holder in enforcing his or her right against infringers, even going as far as to cut entirely one of its own customers from the service (Internet connection) it delivers to him or her. Even more, the access provider could be asked to refrain from re-entering into a new contract with the infringing user either for a limited or an unlimited period of time. Furthermore, as the current practice of website blocking shows, a right holder might apply for such injunctions against all the access providers in one country (country-wide) or in several countries (cross-border),[58] thus effectively precluding a user's possibility to contract the Internet access on his or her own behalf. As a study case, we will consider now the injunctive relief granted in a recent Spanish case.

2 Disconnecting an Alleged File Sharer from the Internet: *Promusicae v. R*

A recent case in Spain, *Promusicae et al. v. R Cable y Telecomunicaciones Galicia*,[59] provides an illustrative example of private litigation seeking an injunction against innocent intermediaries as a means to stop third-party copyright infringement. The concerned ISP was enjoined by the Barcelona Court of Appeal to suspend the provision of Internet access to one of its subscribers, allegedly engaging in P2P file sharing. The case is the first in Spain and probably one of the first in Europe[60]

[55] As mentioned in the introduction of this part, by secondary liability we mean only tort liability of somebody else than of a direct infringer.

[56] *See* Husovec (2013), p. 118, p. 124.

[57] *See more* on website blocking injunctions; Husovec (2013), Feiler (2012), Savola (2014).

[58] *See more* in Savola (2014).

[59] *Promusicae* et al *v. R Cable y Telecomunicaciones Galicia, SA*, Barcelona Court of Appeals, Judgment 470/2013, 18 December 2013.

[60] Finish courts have considered privately litigated disconnections before, Helsinki District Court, Judgment H 08/3008, 23 June 2008 and 6 August 2008; Helsinki District Court, Judgment H 11/11018, 11/11063, 11/11065, 31 March 2011, 9 May 2011 and 21 July 2011 (both courts were reported to allow them as proportionate. *See more* Savola (2013), at 154–156.)

where the provision set out in Art. 8(3) of the InfoSoc Directive has been applied to order the disconnection of an individual – rather than a website – from the Internet.[61]

2.1 Factual Background

The legal action was initiated by Promusicae – a Spanish association of music producers – and the main music labels established in Spain. In its efforts to fight illegal file sharing, Promusicae had hired the investigative firm DtecNet. By monitoring the net, they found that a user of the P2P network Direct Connect, with the nickname "nito75", was making available 5,097 audio files from his or her computer's shared folder. DtecNet actually downloaded three of those files, as evidence to use in court, which indeed corresponded to sound recordings owned by members of Promusicae. In this operation, DtecNet was able to detect the IP address of the user, which had been allocated to that user by R, a small ISP operating in Galicia, in the northwest of Spain.[62] However, knowing the user's IP and the ISP who had allocated it is not enough to initiate a civil legal action against the infringer. Rather, for a right holder to file a complaint against an Internet user, it needs to know who that person is.

Promusicae was well aware that the ISP could not be obliged to reveal the identity of the user. It was not the first time Promusicae had gone after an individual file sharer. Back in 2005, Promusicae went to court to oblige the ISP Telefónica to disclose the identity of some of its users allegedly engaging in copyright infringing file sharing using the KaZaA software, so that it could then bring a civil lawsuit against them. Under the Spanish legislation at that time, however, a user's identity could only be revealed by ISPs in the context of a criminal investigation or for purposes of safeguard public security and national defence, and not for the purposes of civil procedures such as a copyright infringement claim.[63] Thus the court decided to ask the CJEU whether that limitation was in fact permitted under the EU Law, in particular considering the E-Commerce, InfoSoc and Enforcement Directives, and the Charter. The case was *Promusicae v Telefónica*.[64] As it is well known, the CJEU answered that the said limitation is not against the EU Law. The court noted that while Directive 2002/58 does not preclude the possibility for Member States of

[61] We are considering here the disconnection of an individual who is using his or her Internet connection to engage in peer-to-peer file sharing, rather than the case of disconnecting a server offering illegal content. While some of the issues may be similar in both cases, since in both of them a termination of a subscriber occurs, bringing an action seeking to terminate Internet access of a private user shows a particular enforcement strategy, very different from that of going against publicly accessible websites. To be sure, there have been examples of the latter, such as the TDC case in Denmark. In that case, decided by the Danish Supreme Court on 10 February 2006, the Internet access provider TDC was enjoined from transmit infringing works from two FTP servers (xtdck.no-ip.org and scandi.myftp.org) to which it was providing Internet access, and the only way to comply with the injunction was to terminate their connection. *See* Jakobsen (2011a).

[62] *See* http://www.mundo-r.com.

[63] This was established in Art. 12 of Law 34/2002 on information society services and electronic commerce, which was in force at relevant time, and was based in Art. 15(1) Directive 2002/58.

[64] Case C-275/06, *Promusicae v. Telefónica*, judgement of 29 January 2008.

obliging ISPs to disclose personal data in the context of civil proceedings, they are not obliged to impose such an obligation either.[65]

Not being able to find out the identity of the person behind the nickname nito75, a lawsuit against that individual was barred. Hence, Promusicae decided to make use of the redress provided for in the national implementation of Art. 8(3) of the InfoSoc Directive, which, as noted above, directs Member States to ensure that right holders may apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

The conditions and modalities relating to such injunctive relief, as already pointed out, are left to national law.[66] Hence it will be useful to provide a brief summary of how these injunctions are set forth under Spanish law and which are their essential elements and requirements.

2.2 Spanish Legal Framework

The Spanish Copyright Law (LPI) was amended in 2006 to transpose the Copyright and the Enforcement Directives. The injunction provided for in Art. 8(3) of the InfoSoc Directive was introduced in Arts. 138(III), 139(1)(h) and 141(1)(6) of the LPI. In these provisions, the LPI allows right holders to apply for such an injunction against intermediaries, either as a definitive or a precautionary measure, even where the acts of the intermediaries as such are not infringing. Article 138(III) LPI states that

> Both the specific cessation measures contemplated in Article 139(1)(h) and the precautionary measures provided for in Article 141(1)(6) may be requested, when they are appropriate, against the intermediaries whose services are resorted to by a third party to infringe intellectual property rights recognized by this law, even though the intermediaries' acts do not constitute an infringement in themselves, without prejudice to what is established in the Law 34/2002 of 11 July on information society services and electronic commerce. Such measures must be objective, proportionate and non-discriminatory.

Both Art. 139(1)(h) and Art. 141(1)(6) LPI provide for that injunction using identical language – the former refers to it as a definitive measure, and the latter as a precautionary one. In both provisions, the wording describing the measure that right holders may apply for is as follows: "The suspension of the services provided by intermediaries to third parties who avail themselves of them to infringe intellectual property rights, without prejudice to what is established in the Law 34/2002 of 11 July on information society services and electronic commerce."

Some key elements of this legal regime may be highlighted. First, no direct or secondary liability is required on the part of the intermediary. It is expressly established in Art. 138(III) LPI that the injunction will be available even where the intermediary's acts are not in themselves infringing. While this refers to direct

[65] *See id.*, especially paras. 54, 55, 58, 59.

[66] *See* Recital 59 of the InfoSoc Directive.

liability, there is no provision requiring the provider to be secondarily liable either. As noted above, requiring either direct or secondary liability could in some cases restrict the availability of the injunctions too much, thus running afoul of the InfoSoc Directive.

Second, the relationship between injunctive relief and the safe harbours protection has been the subject of some debate in Spanish legal literature and case law.[67] As we have seen, the LPI declares that the availability of the injunctive relief will be "without prejudice to what is established in the Law 34/2002 of 11 July on information society services and electronic commerce." This Law – the LSSICE – constitutes the transposition of the E-Commerce Directive, and implements the Directive's safe harbours shielding intermediaries from liability.[68] One interpretation of this provision concludes that where an intermediary qualifies for one of the LSSICE safe harbours, it is shielded as well from claims for injunctions.[69] However, such a construction is hardly tenable. The LSSICE itself says nothing suggesting that it rules out injunctions against intermediaries protected by the liability exemptions; on the contrary, it remains silent on this point. In addition, as already pointed out, all the safe harbour provisions in the E-Commerce Directive expressly state that they "shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement".[70] A more sound national interpretation, thus, concludes that the "without-prejudice-to" clause simply reminds that the possibility of applying for an injunction does not undermine the protection from liability granted by the safe harbours, which does not extend to shelter intermediaries from injunctions.[71] More importantly, it can be seen as well as a reminder that injunctions against intermediaries cannot entail a general obligation "to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity", which is clearly forbidden by Art. 15 of the E-Commerce Directive.[72]

As to the modalities and conditions of the injunctions, the LPI expressly provides that the relief may be asked either as a preliminary injunction or as a definitive measure. When the plaintiff is applying for a preliminary measure, the basic requirements of *fumus boni iuris* and *periculum in mora* must be satisfied. The law allows the precautionary measure even before the infringement, if there is a sound and rational risk of an imminent infringement.[73]

[67] *See* Garrote (2007).

[68] The LSSICE safe harbours closely follow those in the Directive, with some differences regarding the concept of knowledge, and with the addition of a safe harbour for information location tools.

[69] This reading was held by a lower court in a case of hosting, but it was reversed on appeal. *See Telecinco v. YouTube*, judgement No. 11/2014, Madrid Court of Appeal, 14 January 2014.

[70] *See* Arts. 12(3), 13(2) and 14(3) Directive 2000/31.

[71] Both the InfoSoc and the Enforcement Directives note that their provisions do not affect those of E-Commerce Directive. *See* Recital 16 of the InfoSoc Directive and Recital 15 of the Enforcement Directive.

[72] *See Scarlet*, C-70/10, para. 34.

[73] *See* Art. 141 LPI.

In addition, the LPI establishes that these injunctions can only be applied for where appropriate, and that they must be objective, proportionate and non-discriminatory.[74] These open-ended requirements should allow courts to consider all the circumstances of the case and to assess whether, in such circumstances, granting the injunction would be excessive.

Finally, as to the contents of the injunctions, they consist of ordering the intermediary to suspend the service it provides to the infringing party, which in the case of access services might entail the disconnection of the subscriber. Regarding the time extension, by its very nature, preliminary injunctions will be time limited. On the contrary, when the injunction is granted as a definitive measure it may or may not be subject to temporary limits.

2.3 The Ruling

Under the above-summarized legal framework, Promusicae and the other plaintiffs lodged its complaint exclusively against the ISP, asking the court to enjoin it, immediately and permanently, from providing Internet access to the alleged infringer, that is, to the person who was allocated the specified IP address at the relevant time. However, the ISP did not answer the complaint, and thus the lower court decided the case without its participation. The lower court denied the injunction holding that the acts of the user were not infringing.[75] Plaintiffs appealed and, again, the defendant ISP chose not to respond before the court. The appellate court finally granted the claimed injunction.

In its ruling, the appellate court acknowledges that the Spanish Copyright Act provides for an injunction against an intermediary whose services are being used by third parties to infringe copyright and related rights. It further asserts that providers of access and transmission services do hold standing to be sued for such an injunction even where they are exempted from liability under the mere conduit safe harbour set forth in Art. 14 of the Spanish Law on Information Society Services.[76]

Then the ruling turns to the question of whether the acts allegedly carried out by the user were infringing, as the underlying infringement is a condition for the injunction to be granted. Relying on the evidence produced by the plaintiffs, the court considered it proved that the user by the nickname of *nito75* was actually making 5,097 sound recordings available through the P2P network. The court found that this constitutes an infringement. First, putting a copy of the sound recording in the shared folder involves an act of reproduction not covered by the private copy exception, as that use cannot be considered private. Second, making the files accessible through the P2P network constitutes an act of making the concerned

[74] *See* Art. 138 LPI.

[75] The ruling, however, is notoriously flawed in this regard as it describes the user's activity as if it were the administrator of a linking website, which had nothing to do with the actual facts.

[76] This provision transposes almost verbatim the liability exemption laid down in Art. 12 of the E-Commerce Directive. *See* the discussion above regarding the availability of injunctions against intermediaries exempted from liability.

phonograms available to the public – an exclusive right that belongs to the producer of the phonograms.[77]

Having determined that the ISP was providing access to an unknown user who was directly infringing the plaintiffs' rights, the court decided to grant the claimed injunction ordering the ISP to no longer provide Internet access to that user. No objections to the issuing of the injunction were discussed in the ruling – perhaps, in part, due to the fact that the defendant ISP decided not to respond and never showed up in court. Remarkably, there is no assessment whatsoever of the issue of proportionality in the ruling. There is no discussion of whether or not the one who will actually be affected by the injunction, i.e. the user who is going to lose access to the Internet access, should be heard before granting the injunction – indeed, the user was never part of the proceedings, as the complaint was lodged only against the ISP.

Likewise, there is no reference in the ruling to the fact that an IP address does not tell us who the infringer is. An IP address – plus the date and time frame – allows the ISP to identify a particular subscriber of its access services – the one to whom that particular IP address was allocated at that time. But this doesn't mean that precisely that subscriber is the one who carried out the infringing acts. Different people within the subscriber's family entourage might have used that IP to navigate the Internet. In case of a non-protected wifi connection, a number of persons within the area might have been using it.

Beyond the noted shortcomings of the ruling, we can wonder about the effectiveness of such an order. The legal proceedings started on 13 December 2010, when the plaintiffs' lodged the complaint against the ISP. The appellate court issued its ruling ordering the injunction on 18 December 2013. Such a long period of time renders the injunction useless.[78] If nothing else, the ISP was no longer keeping the records of the IP addresses it allocated its customers three years before.[79] Actually, immediately after the ruling, the concerned ISP declared in a press release that it would not be able to identify the subscriber and that complying with the injunction was therefore impossible.[80]

As was shown above, the practical execution of a disconnection injunction heavily depends on the ISP's data retention periods and sometimes also on the possibility to oblige the ISP to disclose the identity of the alleged infringer. Both issues are probably as highly contentious in the European debate[81] as user disconnections themselves.

[77] *See* Art. 3(2)(b) InfoSoc Directive and Art. 116 of the Spanish Copyright Act (LPI).

[78] Unless a preservation order is granted in parallel.

[79] Even the way of ordering the injunction is surprising. The court directs the defendant ISP to "suspend immediately and definitively the provision of internet access to the user that utilizes the nickname *nito75*." This is surprising because that nickname means nothing to the ISP. That was just the nickname the file sharer used in the P2P network, not a user name as an ISP's customer. In order to precisely identify the user, what the ISP needs is their IP address (which was indeed mentioned in the complaint) and the precise date and time.

[80] *See* http://quecheparece.blogs-r.com/weblog/ver-post/sobre_a_sentenza.

[81] *See* the line of cases *Promusicae* C-275/06, *Tele 2* C-557/07, *Bonnier Audio* C-461/10, a line that was further developed recently by a landmark decision of the CJEU in *Digital Rights Ireland* C-293/12, which invalidated the Data Retention Directive.

3 Discussion

Privately litigated Internet disconnection injunctions such as one granted by the Spanish court pose many problematic issues. In this part we discuss some of these problems, focusing on the issues of fair trail, "quality of the law" and proportionality.

3.1 Right to a Fair Trial

The Spanish court ordered the disconnection of a user who was not part of the proceedings. The only defendant – an access provider – did not object or respond to any of the plaintiff's submissions. In this scenario, even more than in the case of website blocking injunctions,[82] it is very doubtful that the user's fundamental right to a fair trial under both Art. 6(1) of the Convention and Art. 47 of the Charter was respected at all. According to the ECtHR,[83] everybody shall be afforded a right to fair trial as long as the outcome of the case is "*decisive* for private rights and obligations".[84] For the CJEU, this must be the case when "interests [of a person] are perceptibly affected".[85] Is cutting off somebody from Internet access a decisive or perceptible outcome in this sense?

It can be argued that a disconnection injunction leads to proceedings that are no different from any regular enforcement of rights against elements of the infringement channel such as distributors, importers or technical manufacturers. In these cases we often do not require a presence of the actual producer who is inevitably also affected by the outcome. Thus in such cases the negative direct consequences per se do not justify a need for a full inclusion of the producer in the lawsuit. This seems right. Due process guarantees should be only triggered if the outcome has some more intensive impact. ECtHR case law employs this filtering mechanism under considerations of "genuine and serious dispute".[86] Disconnection is such a serious dispute not only because it affects more interactions in the course of daily life than an injunction against a single distributor, but mostly because future substitution of providers on the market is usually more limited than of distributors.

Under the Strasbourg case law, the right to a fair trial has two main components, namely: (i) the right to have access to the court, and (ii) equality of arms. According to the ECtHR, the latter principle requires that each affected party is afforded a reasonable opportunity to present its case, including its evidence, under conditions

[82] *See* for a critique Husovec (2013), p. 121 et seq.

[83] The Convention applies more relaxed standards to "private rights and obligations" than to "any criminal charge" (*Dombo Beheer B.V. v. The Netherlands*, App. No. 14448/88, para. 32). Some of the standards are, however, applied similarly also in the civil context (*Vanjak v. Croatia*, App. No 29889/04, para. 58). For a discussion on whether a disconnection could be seen as a criminal charge within the autonomous meaning of Art. 6 of the Convention, *see* below.

[84] *See* ECtHR, *Ringeisen v. Austria*, App. No. 2614/65; the scope of the Charter is even broader in this respect (*see* Weiß (2013), p. 288).

[85] *See* CJEU, Transocean, Case 17/74, para. 15.

[86] *See* ECtHR, *Krosta v. Poland*, App. No. 36137/04, para 50.

that do not place it at a substantial disadvantage vis-à-vis its opponent.[87] Also the CJEU noted in a different context that "a person whose interests are perceptibly affected by a decision taken by a public authority *must be given the opportunity to make his points of view known*".[88] In addition, the CJEU explicitly requires in its pre-Charter case law that public authorities adopting a decision must provide the affected persons a possibility to be heard,[89] because the right to be heard is the essence of the due process guarantees. The extension of this rule can be also found in Art. 41(2) of the Charter, which establishes "[the] right of every person to be heard, before any individual measure which would affect him or her adversely is taken".

The Spanish user whose disconnection was ordered, did not have any possibility to defend himself as to (i) the occurrence of an alleged infringement, (ii) the validity and legality of the evidence that was submitted to the court, and (iii) the proportionality of the disconnection as such. It is difficult to understand how a user who was never notified about "his case", could still somehow preserve a possibility to comment on all the evidence adduced or observations filed, with a view to influencing the court's decision.[90] The issues a user may raise in this type of litigation are far from theoretical:

- What if the one who committed the infringement was not a customer of the ISP, but someone else who used the user's IP address? (e.g. his children, spouse or an unrelated user of his open wifi);
- What if the subject matter that was shared already fell outside of copyright protection or was covered under some of the exceptions?
- Can the plaintiff still invoke his claims before the courts (e.g. due to prescription)?
- Was all the evidence presented to the court valid and admissible?[91]
- Based on circumstances of that user, is it proportional to disconnect him from the Internet, which might be essential for his personal and professional life?

[87] *See* ECtHR, *Ankerl v. Switzerland*, App. No. 17748/91.

[88] *See* CJEU, *Transocean*, Case 17/74, para. 15.

[89] *See* the decision of the CJEU, *Ismeri Europa Srl v. Court of Auditors*, C-315/99 P: "Although the adoption and publication of reports of the Court of Auditors are not decisions directly affecting the rights of persons mentioned therein, they are capable of having consequences for those persons such that those concerned must be enabled to make observations on those points in such reports which refer to them by name, before those reports are definitively drawn up".

[90] *See* ECtHR, *J.J. v. The Netherlands*, App. No. 21351/93 and *Ferreira Alves v. Portugal*, App. No. 25053/05.

[91] Even the issue of admissibility of evidence could be potentially an issue of the Union law; *see* CJEU, *Joachim Steffensen*, C-276/01 ("the national court must verify that the national rules on the taking of evidence applicable to such an action are not less favourable than those governing similar domestic actions (the principle of equivalence) and that they do not render practically impossible or excessively difficult the exercise of rights conferred by Community law (the principle of effectiveness). In addition, the national court must consider whether such evidence must be excluded in order to avoid measures incompatible with compliance with fundamental rights, in particular the right to a fair hearing before a tribunal as laid down in Article 6(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms").

– Is such a punishment, which has the intensity of a criminal penalty (see below), still "prescribed by the law" as required by the Charter and the Convention?
– Why should the court grant such an injunction without any time limit or possibility to review?

All these are legitimate questions, which every defendant, would naturally raise in the main proceedings. The court, by deciding in any of them, inevitably does so based only on the one-sided submission by the plaintiff, who obviously has an interest in the least resistance in the proceedings. It is true that because the plaintiff is *dominus litis*, i.e. the master of the lawsuit, he decides who he wants to name as a defendant. The court, however, as a public authority, should not enter any favorable decision if any of the perceptibly affected parties is somehow unrepresented in the proceedings. Any national court must observe this principle not only as a matter of its own legal tradition and ECtHR case law, but also as a matter of Art. 47 of the Charter, which is applicable in these cases. Otherwise, both the outcome and the procedure leading to it would be in substantial breach of the Union law. As Eleanor Roosevelt once famously said: "Justice cannot be for one side alone, but must be for both". Courts granting Internet disconnection injunctions upon hearing only one party violate this basic proposition of justice.

In addition, the right to be heard is not the only component that is not respected in a litigation like the Spanish one. The user who is potentially cut off from Internet access has also *ex post* no legal means to challenge the decision itself, as he was not party to the proceedings. This raises a question of whether the user's right to access to the court was also fully respected. From the user's perspective, there might well be, depending on the national law, no judicial course of action enabling him to *ex post* revoke the result of the already effective decision between two parties in his own affair, despite the fact that it does not constitute *res judicata* for him.

If the disconnection injunction would be preceded by disclosure of the identity of the user, who would be subsequently named as a defendant along with the access provider, or at least given other procedural possibility to defend his case,[92] the right to a fair trial issues might be mitigated. Still, nevertheless, the question of the proportionality of such measures would remain open.

3.2 Punishment without Law

In the previous due process discussion we assumed that Internet disconnection injunctions are to be treated as a civil matter.[93] However, this is not necessarily always the case. The ECtHR applies so called Engel-criteria[94] in order to determine if the case is a "criminal charge" under Art. 6 of the Convention.

[92] Some courts employ some kind of "reversed due process guarantees" when they grant an injunction, but then allow for a revision upon the objection by those who prove their interest. The CJEU itself used similar mechanism to guarantee freedom of expression in its *UPC Telekabel Wien* decision (para. 57).

[93] Indeed if the proceedings that result in an Internet disconnection injunction would be qualified only as a civil issue, then Art. 7 of the Convention would not apply (*Kot v. Russia*, App. No. 20887/03, para. 38), and the ambiguous legal basis could only be addressed within the proportionality exercise.

[94] *Engel and other v. The Netherlands*, App. No. 5100/71.

Those criteria are: (a) the classification in the national law, (b) the nature of the offence, and (c) the possible punishment. Whereas the criterion (a) only serves one-way into the autonomous term;[95] criteria (b) and (c) are alternative.[96] Therefore it is possible that, even if the national law imposes a certain sanction as a matter of civil law, it would be qualified as a "criminal charge" under Art. 6 of the Convention. Because some of the disconnection injunctions can arguably be more preventive-repressive than corrective (b) and the sanction can be very serious (c), it could be potentially qualified as a "criminal charge" for the purposes of the Convention.[97] This has very important consequences, because the *nulla poena sine lege* principle of Art. 7 of the Convention would then automatically apply.[98]

This rule should arguably require stronger "quality of the law" (*nullum poena sine lege certa*) than that required by the Convention in the context of balancing interferences with the conflicting human rights. The application of this rule poses the question of whether a sanction of disconnection[99] based on a literal implementation of Art. 8(3) of the InfoSoc Directive such as Spanish one, can be said to be predictable enough to satisfy this rule. Especially given the fact that the provision is directed at intermediaries, which makes it difficult to infer that it can give rise to any so serious sanction against the infringer himself. If the intensity of the disconnection is strong, either due to its temporal length, scope or other consequences, it is submitted that the verbatim national implementation of Art. 8(3) of the InfoSoc Directive alone will not satisfy the conditions of Art. 7 of the Convention.[100]

3.3 Restrictions on Fundamental Rights

If the injunction sought would effectively achieve the goal of depriving an individual of his or her Internet connection, it would certainly comport serious restrictions on that user's fundamental rights, particularly on the right to freedom of expression.

The 2009 revision of the Telecom Package amended the Framework Directive[101] to include particular safeguards with regards to national measures limiting access to end-users to the Internet. New Art. 1(3a) of the Framework Directive explicitly states that any such measure taken by Member States "shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention

[95] If the national law classifies it as a criminal charge, then so does automatically the Convention.

[96] *See more* in Grabenwarter (2014).

[97] *See Albert v. Romania*, App. No. 31911/03, *Žugić v. Croatia*, App. No. 3699/08, *Thomas v. France*, App. No. 12821/01.

[98] *Paksas v. Lithuania*, App. No. 34932/04. *Cf.* Art. 49 of the EU Charter.

[99] *Kafkaris v. Cyprus*, App. No. 21906/04, para. 150.

[100] On Art. 7 "quality of the law" context; *see more* in Grabenwarter (2014), pp. 178–181.

[101] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (hereinafter "Framework Directive").

for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law."[102] It establishes, moreover, that

> any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may *only* be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process.[103]

As the ECtHR noted in *Yildirim v. Turkey* in 2012, "the Internet has now become one of the principal means by which individuals exercise their right to freedom of expression and information, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest".[104] In a similar vein, the French Constitutional Council held in 2009 that "[i]n the current state of the means of communication and given the generalized development of public online communication services and the importance of the latter for the participation in democracy and the expression of ideas and opinions, this right implies freedom to access such services".[105] Being banned from access to the Internet affects particularly the freedom to receive and impart information and ideas, which is an integral part of the right to freedom of expression.[106]

Both under the Charter and the Convention, restrictions on those rights are only acceptable when they are predictable, justified and proportionate. According to the Charter, any restriction must be (a) provided by law, and (b) respect the essence of the rights and freedom to which the restriction affects.[107] In addition, "[s]ubject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."[108] Thus, injunctions which do not pass this test would go beyond the maximum ceiling allowed under Art. 8(3) of

[102] Article 1(3a) Framework Directive, as amended by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services (Text with EEA relevance).

[103] *Id.* (emphasis added).

[104] ECtHR (2nd Section), 10 December 2012, *Yildirim v. Turkey* (App. No. 3111/10), para. 54.

[105] *See Conseil Constitutionnel,* Decision no 2009-580 DC, 10 June 2009 (English translation available at http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank_mm/anglais/2009_580dc.pdf).

[106] *See* Art. 11 of the Charter. *See also* ECtHR (2nd Section), 10 December 2012, *Yildirim v. Turkey* (App. No. 3111/10), paras. 50–55. Other rights, such as users' privacy or the ISP's freedom to conduct a business are also liable to be affected.

[107] *Cf.* Art. 52(1) of the Charter.

[108] *Idem.* The Convention offers specific tests for different rights, requiring the restriction to be provided by law and to be necessary in a democratic society in the interests of some general interests, including for the protection of rights of others. *See*, for instance, Art. 10 of the Convention.

the InfoSoc Directive, as already noted above. This was recently stressed also by the *EU Human Rights Guidelines on Freedom of Expression Online and Offline (Guidelines)*[109] in the context of website blocking injunctions:

> Blocking access to websites on the grounds of copyright protection could constitute a disproportionate restriction of freedom of opinion and expression. Any restrictions must comply with the three part cumulative test set out in paragraph 20 of these Guidelines [(a) principle of legal certainty, predictability and transparency, (b) principle of legitimacy, (c) principles of necessity and proportionality].

This test resembles the standard test employed often by the CJEU in its case law. However, there are some slight differences, which we will contrast below.

3.3.1 A Measure Prescribed by the Law: Legal Certainty, Predictability and Transparency

The starting point in the analysis – whether Internet disconnection injunctions are prescribed by law, meeting the principles of legal certainty, predictability and transparency – will depend on the way Art. 8(3) has been implemented into the national law of the concerned Member State.

The InfoSoc Directive does not prescribe that such injunctions must be implemented only as civil law claims, but also as administrative or other measures.[110] Article 8(3) does not explicitly provide for an injunction consisting precisely of the disconnection of an allegedly infringing user. Nonetheless, as already noted, the CJEU construes Art. 8(3) in a broad manner, clearly encompassing access providers within its scope.[111] The CJEU has so far analyzed different kinds of injunctions against ISPs under Art. 8(3), namely, injunctions ordering access providers to filter and block the P2P traffic of all its customers[112] or to block access to an infringing website.[113] Taking into account the InfoSoc Directive's goal of providing a high protection for copyright owners, and the wording of its Recital 59, referring to the possibility of injunctions "against an intermediary who carries a third party's infringement of a protected work or other subject-matter in a network", it appears that an injunction to terminate a subscriber account would in general be deemed to fall within the scope of Art. 8(3).

[109] Council of the European Union (2014). EU Human Rights Guidelines on Freedom of Expression Online and Offline. http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf. Accessed 22 August 2014.

[110] It is submitted that national legislation providing for administrative graduate response schemes which impose some duties on the ISPs to prevent, or to put an end to, an infringement may also be seen as implementing Art. 8(3) InfoSoc, and thus subject to the Charter standards.

[111] *See Telekabel*, C-314/12 para. 33 ("To exclude internet service providers from the scope of Article 8(3) of Directive 2001/29 would substantially diminish the protection of rightholders sought by that directive"). *See also Tele 2*, C-557/07, para. 45.

[112] *See Scarlet*, C-70/10.

[113] *See Telekabel*, C-314/12.

Thus, a verbatim national implementation of Art. 8(3) would probably comply with the requirement that the restriction is prescribed by law. Conversely, a very cumbersome and complicated injunction might lack the needed legal base, and a very simple one might also be devoid of legal support if it is not a predictable outcome in view of the national legislation.[114]

3.3.2 Legitimacy

Turning to the purposes of the injunction, there is little discussion that it seeks legitimate interests, specifically that of protecting intellectual property rights, expressly protected by the Charter (Art. 17).

3.3.3 Principles of Necessity and Proportionality

The question arises as to whether disconnection injunctions are necessary to protect the intellectual property rights. That is, (a) whether the same result could be reached by less intrusive means, and (b) whether the measure can be deemed effective in achieving its goal. Furthermore, even if the injunction were indeed necessary for the intended objective, it still should be considered if the restrictions caused by such measure are proportionate to the relevance of the results pursued.[115]

The question of (a) whether there are other, less restrictive means available in order to reach the goal of putting an end to the infringement, can be seen from two different perspectives, namely, from the standpoint of the burden imposed on the ISP and from the perspective of the restriction of the user's rights. From the former point of view, suing the user directly would avoid impinging on the ISP's freedom to conduct a business and thus could be seen as a less intrusive measure. Nonetheless, even in that case the cooperation of the ISP would be needed to identify the user, whereas, as discussed above, Member States are not obliged to impose on ISPs a duty of revealing a user's identity for the purposes of civil lawsuits. On the other hand, the injunction to cut a subscriber's account may not be that onerous for the ISP after all. As shown by the Spanish study case, the cost for the ISP could be in fact so low that it lacks any incentive to fight such an injunction in court.[116] Finally, the Directive suggests that going against the ISP could be the only realistic solution available.[117] Seen from the point of view of the user, it could be argued that in order to stop the illegal file sharing in which he or she is allegedly engaging, there is no need to completely block his or her access to the Internet;

[114] A great account of the ECtHR case law in this respect is provided by Advocate General Cruz Villalón in Scarlet Extended, who summarizes it as follows: "The 'law' must therefore be sufficiently clear and foreseeable as to the meaning and nature of the applicable measures, and must define with sufficient clarity the scope and manner of exercise of the power of interference in the exercise of the rights guaranteed by the ECHR."

[115] *Cf.* Art. 52(1) of the Charter. *See also* Art. 1(3a) of the Framework Directive, requiring the measure to be both proportionate and necessary.

[116] The situation would of course be different if right holders would decide to apply for a high number of injunctions.

[117] *See* Recital 59 InfoSoc Directive.

rather a more limited measure, such as blocking P2P traffic from and to that IP address would be enough, assuming that such blocking is technologically feasible.[118] Moreover, the above-mentioned Guidelines seem to apply this part of the test even more strictly, requiring the measures to be "the least restrictive means" needed to achieve the purported aim".

As to (b) the actual capability of measures to achieve its aim (effectiveness), a disconnection injunction raises serious doubts. Terminating a subscriber's account would only be effective if maintaining such account were the only way for the subscriber to keep accessing the Internet from his or her personal device. This is obviously not the case, as open wifi areas are now ubiquitous. Access to the Internet is easily found in coffee shops, libraries, airports, commercial centres, universities and many other public spaces. To be sure, however, none of those is an exact equivalent to accessing the Internet from home. Interestingly, the French Constitutional Court's decision on the HADOPI Law noted that the envisaged suspension would entail a restriction of "the right of any person to exercise his right to express himself and communicate freely, *in particular from his own home*."[119] Accessing the Internet from home may, in addition, be particularly relevant in some situations – working from home, access to online education, etc.

On the other hand, in most cases a subscriber might easily shift to a different provider,[120] even before the court issues the injunction. All in all, terminating the subscriber's access account is hardly a guarantee that the infringement will cease because the user will no longer be able to access the Internet.[121] Nor it is likely to function as a deterring weapon that will be able to curb online piracy. Nonetheless, it is submitted that even if the user may find alternative ways to access the net, being cut from his or her access provider arguably results in a serious limitation to their rights.

At the same time, it is likely that the CJEU will be nevertheless satisfied even by this negligible capability of the injunctions given that according to its case law, even measures that do not properly achieve intended purpose might be justified.[122] The CJEU's attitude of accepting everything but "manifestly inappropriate"[123]

[118] Even this would of course entail blocking legitimate traffic, for instance, services relaying on P2P protocol, such as Skype, or Spotify, or the transmission of non-copyrighted files via P2P. Nonetheless, the restriction would be certainly less burdensome for the user.

[119] *See* para. 16.

[120] A different scenario would be that were all the access providers in the country were enjoined from providing their services to the allegedly infringer. Still, this person could easily circumvent such a general prohibition, for instance using someone else's connection.

[121] Of course, the argument works also the other way: the less likely the is user to suffer a real isolation from the Internet, the lower will be the restriction on his right to freedom of expression and access to the information. See Strowel (2009), at 82.

[122] In the context of website blocking, the CJEU has held that the blocking measures "must have the effect of preventing unauthorised access to the protected subject-matter or, at least, of making it difficult to achieve and of seriously discouraging internet users who are using the services of the addressee of that injunction from accessing the subject-matter made available to them in breach of that fundamental right". *See UPC Telekabel Wien*, C-314/12, para. 63.

[123] *See*, *e.g. Vodafone and Others*, C-58/08, para. 52.

measures capable of achieving a certain goal seems, however, to be a part of a bigger external inconsistency of the CJEU case law tool kit with that of ECtHR.[124]

Even if the injunction were to be deemed necessary, it would still need to be justified as proportionate in light of the aim pursued. Suspending the Internet connection not only prevents the user from using it to infringe copyright, but prevents her as well from carrying out a wide range of lawful acts. Particularly, as in the website blocking cases, the user also loses access to lawful information, and thus the injunction goes beyond its purpose – it over-blocks.[125] Furthermore, as noted above, the IP address does not identify the particular person who is using it. It only identifies a provider's subscriber – who may be either an individual or a company. The same IP address may have been used by a number of persons – employees of the company, the subscriber's family members, neighbours, etc. Thus, cancelling that access is liable to affect several people not at all involved in the alleged infringements. Taking into account the nature of the rights that are restricted by the suspension, and the fact that not only the alleged infringer but also other people might be affected by it, it is rather dubious that such an injunction would respect the principle of proportionality.[126] This lack of proportionality is all the more clear when the injunction is not limited to a certain period of time. At the very least, the injunction would not only need to be targeted at a specific online activity, be adequately limited in time and subject to other safeguards, but also would need to take into account all the circumstances of the defendant such as the importance of the Internet for his private and professional life. Compared to the case of website blocking injunctions, where open-ended measures have been considered acceptable,[127] any disconnection injunction measure should be strictly defined to guarantee that the *user's* and not only ISP's rights are taken into account.

[124] Weiß (2013), p. 290. It would be worth to look into *internal consistency* of the CJEU case law in this respect as well, given that the test in various decisions does not seem to always build a coherent framework.

[125] *See Telekabel*, C-314/12, para. 56 (stating, in the context of website blocking, that the measure "must serve to bring an end to a third party's infringement of copyright or of a related right but without thereby affecting internet users who are using the provider's services in order to lawfully access information. Failing that, the provider's interference in the freedom of information of those users would be unjustified in the light of the objective pursued"). *See also* the ECtHR ruling in *Yildirim v. Turkey*.

[126] In his report to the UN Human Rights Council on the promotion and protection of the right to freedom of opinion and expression, Special Rapporteur Frank La Rue considered that "cutting off users from Internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law [is] disproportionate and thus a violation of article 19, paragraph 3, of the International Covenant on Civil and Political Rights", and urged States "to repeal or amend existing intellectual copyright laws which permit users to be disconnected from Internet access, and to refrain from adopting such laws." *See* Special Rapporteur Frank La Rue, "Report on the promotion and protection of the right to freedom of opinion and expression", Human Rights Council, U.N. Doc. A/HRC/17/27 (16 May 2011) p. 21, available at http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

[127] *UPC Telekabel Wien*, Austrian Supreme Court (OGH), Judgment 4 Ob 71/14 s, 24 June 2014 (comes to conclusion that under the Austrian law, *only* general injunctions not specifying the instruments can be granted). It must be noted that the CJEU did *not* mandate open-ended measures (website blocking injunctions), but only enabled them under some circumstances; *see* more discussion in Husovec (2014).

4 Conclusion

The scope of the injunctions against intermediaries as construed by CJUE case law is potentially very broad, particularly as regards the notion of an intermediary, and it is certainly not limited by the liability exclusions laid down in the Electronic Commerce Directive. While the specific conditions for the injunctions are left to national law, there is both a minimum floor of injunctive relief Member States must provide, and a maximum ceiling for the injunctive relief they are allowed to grant. To a large extent, this maximum ceiling is determined by human rights limits. Indeed, the Union's human rights standards greatly limit the possibility of many of these types of injunctions. Not only courts, but also Member States themselves are limited by the Charter in the discretion they enjoy with regards to the way of implementing and interpreting Art. 8(3) InfoSoc Directive.

In particular, the injunctions consisting of requiring ISPs to cease providing Internet access to one of their subscribers raise serious concerns from the standpoint of their compatibility with the EU Charter of Fundamental Rights and the European Convention of Human Rights, even where their effectiveness is low because the user may shift to a different provider, or access the Internet from a public place. For these injunctions to be compatible with the Charter and the Convention, they should respect a number of key requirements. First, as discussed in Part 3(1), the concerned individual should be granted the opportunity to defend his or her rights in court. To this end, the plaintiffs would need to previously identify that user, so that he or she could be included in the lawsuit. Second, as shown in Part 3(2), some injunctions, particularly those without time limits, those targeting all national ISPs, or blocking also legitimate communications, might qualify as a criminal sanction and hence be unavailable due to the requirement of a stricter legal basis for criminal charges. Third, as explored in Part 3(3), the test of proportionality seems difficult to be complied with. At the very least, the injunction should be narrowly tailored and show a sufficient degree of effectiveness.

These problems make it extremely complicated that these injunctions are granted if courts, as they must, demand that the injunction applied for complies with the principles enshrined in the Charter and the Convention. In any event, obtaining such an injunction would be costly and slow for the plaintiff, and the outcome would hardly be effective in bringing to an end the user's infringing activity. While some right holders may be inclined to explore these injunctions on the basis of the national transpositions of Art. 8(3) InfoSoc Directive, it seems unlikely that this form of relief may end up being an attractive and effective tool to curb online infringement.

References

Angelopolous Ch (2009) Filtering the internet for copyright content in Europe. IRIS Plus, p 5

Bridy A (2012) Graduated response American style: "six strikes" measured against five norms. Fordham Intellect Prop Media Entertain Law J 23(1):1–66

Czychowski Ch, Nordemann J (2013) Grenzenloses Internet: entgrenzte Haftung? GRUR. 986
Dinwoodie G (2014) Secondary liability for online trademark infringement: the international landscape. Columbia J Law Arts: vol. 36; Oxford legal studies research paper no. 23/2014, p 16
Feiler L (2012) Website blocking injunctions under EU and US Copyright law: slow death of the global internet or emergence of the rule of national copyright law? TTLF working paper no 13
Garrote I (2007) La suspension cautelar o cesación definitive de los servicios a los usuarios infractores de derechos de propiedad intellectual, 27 pe.i. *Revista de propiedad intelectual* 13–55
Giblin R (2014) Evaluating graduated response. Columbia J Law Arts 37:147–210
Gilles S (1992) Negligence, strict liability, and the cheapest cost-avoider. Virginia Law Rev 78(6):1295
Grabenwarter Ch (2014) *European Convention on Human Rights* – Commentary. C.H.Beck, Hart, Nomos, Helbing Lichtenhahn Verlag, Munich, p 111
Grabenwarter Ch, Vranes E (2013) Kooperation der Gerichte im europäischen Verfassungsverbund: Grundfragen und neuste Entwicklungen. Manzsche Verlags- und Universitätsbuchhandlung, Vienna, p 15
Halldórsdóttir H (2004) Enforcement of copyright. Scand Stud Law 47:168
Husovec M (2013) Injunctions against innocent third parties: the case of website blocking. JIPITEC 2:116–129
Husovec M (2014) CJEU allowed website blocking injunctions with some reservations. J Intellect Prop Law Pract 9(7):631–634
Jakobsen S (2011a) Injunctions against mere conduit of information protected by copyright: a Scandinavian perspective. Int Rev Intellect Prop Compet Law (IIC) 42:151–180
Jakobsen S (2011b) Mobile commerce and ISP liability in the EU. Int J Law Inf Technol 1:46
JHR and LB (2013) After Åkerberg Fransson and Melloni. Eur Const Law Rev 9:170–172
Koziol H (2012) "Providerhaftung nach ECG und MedienG" in: Berka W, Grabenwarter Ch, Holoubek M (eds.) *Persönlichkeitsschutz in elektronischen Massenmedien* Manz Verlag
Laffranque J (2012) Who has the last word on the protection of human rights in Europe? Juridica International. vol XIX
Leistner M (2014) Structural aspects of secondary (provider) liability in Europe. J Intellect Prop Law Pract 9(1):75–90
Mayr S (2013) Putting a leash on the Court of Justice? Preconceptions in national methodology v effet utile as a meta-rule. Eur J Legal Stud 5(2):8–21
Meale D (2011) NewzBin2: the first section 97A injunction against an ISP. J Intellect Prop Law Pract 6:854–857
Peguera M (2010) Internet service providers' liability in Spain: recent case law and future perspectives. J Intellect Prop Inf Technol E-Commerce Law (JIPITEC) 1:154
Savola P (2013) Internet-operaattori ja perusoikeudet. In: Tapani L (edw), *Oikeustiede-Jurisprudentia* XLVI, pp 131–221
Savola P (2014) The ultimate copyright shopping opportunity: jurisdiction and choice of law in website blocking injunctions. IIC 45(3)
Seifert A (2011) Die horizontale Wirkung von Grundrechten. Europarechtliche und rechtsvergleichende Überlegungen. Europäische Zeitschrift für Wirtschaftsrecht (EuZW): 18:697
Strowel A (2009) Internet piracy as a wake-up call for copyright law makers: is the 'graduated response' a good reply? WIPO J 1:75–86
Weiß W (2013) Grundrechtssutz durch den EuGH: Tendenzen seit Lissabon. Europäische Zeitschrift für Wirtschaftsrecht (EuZW), p 289–290
Yu PK (2010) The graduated response. Florida Law Rev 62:1374–1430