COMPARATIVE ANALYSIS ON NATIONAL APPROACHES TO THE LIABILITY OF INTERNET INTERMEDIARIES FOR INFRINGEMENT OF COPYRIGHT AND RELATED RIGHTS

Ignacio GARROTE FERNÁNDEZ-DÍEZ[1]
Associate Professor of Civil Law
Autonomous University of Madrid

[1] The author would like to thank Prof. Juan José Marín López, Professor of Civil Law at the University of Castile-La Mancha (Spain), for his generosity when it came to providing a good part of the material used in the research that led to the drafting of this paper. Thanks for their collaboration must also go to Carlos Castro (Colombia), Adriana Mauleón (Mexico), Anastasia Amosova (Russia) and Federico Mastrolilli (Italy). Any possible errors committed in this paper are the author's exclusive responsibility.

TABLE OF CONTENTS

I. INTRODUCTION

This study set out to analyse the liability of Internet intermediaries in cases of copyright and related rights infringement in fifteen different jurisdictions.

For the purposes of achieving this goal, it should be borne in mind that the concept of "intermediary" used in this study encompasses different economic activities.

Firstly, the term includes internet service providers[2] (ISPs),[3] as defined and regulated by different statutory instruments in force, including, in particular, the European Union Directive on Electronic Commerce (hereinafter referred to as the DEC) and the US Digital Millennium Copyright Act (hereinafter referred to as the DMCA).

One is thus speaking here of enterprises that provide services of "mere conduit" or "caching", and "hosting", with this last term strictly referring to those who confine themselves to allocating server space to third parties, without providing additional services.

However, the concept of "intermediary" used in this paper also includes other cases in which there is an activity of direct or indirect collaboration with infringement of intellectual property rights by online end-users.

Hence, the concept of *intermediation* in the widest sense also extends to those who design, maintain and commercially exploit electronic platforms or social networks adapted to Web 2.0. In cases such as these (take, for example, the *Facebook*, *Dailymotion*, *Myspace*, *Twitter*, *YouTube* or *Ebay* services), the work of the electronic-platform owner consists of providing technological and/or economic support to enable the exchange of content matter or its dissemination by third parties.

These activities will be generally referred to as "Web 2.0 intermediation activities" or "Web 2.0 platforms", on analysing whether they are entitled to benefit from the exemption established for hosting by many jurisdictions.

Likewise included in this study are cases such as web pages which contain directories or lists of hyperlinks that direct the end-user to external digital storage sites, or which launch peer-to-peer (P2P) applications that allow end-users to accomplish the exchange of files.[4] These are cases that will be generically classed under the category of "link-listing websites".

This paper will also include another intermediation activity in the broad sense, namely that of Internet search engines which locate and facilitate access to online content via hyperlinks, thereby posing the problem of what happens when such linked material infringes intellectual property rights. In this case, reference will be made to the blanket term, "Internet search engines".

---

[2] For these purposes, it is pertinent to recall the distinction between publishers and intermediary providers (of mere transmission or access, proxy caching, and hosting). In the former case, the ISP has control over the content that it posts online. If, by its conduct, it violates the owners' exclusive rights, it will be held answerable for this in the manner envisaged by the respective enactments and does not enjoy the exemptions from liability (safe harbour) which many such enactments envisage for intermediaries. Where, in contrast, an ISP is carrying out intermediation activities, the safe harbours provided for in the various enactments are applicable, along with the specific requirements and conditions in said laws.

[3] Internet Service Providers.

[4] These pages contain a great number of hyperlinks on which users can click to initiate the file download process by means of P2P programmes.

Lastly, persons who provide online software designed to enable end-users to exchange files by means of P2P technology could also be regarded as "intermediaries", though in this particular case one would have to analyse whether their contribution to the infringement of rights committed by such users indeed sufficed to warrant the description of "intermediary".

Apart from a brief overview, however, this study does not include a detailed analysis of the different "graduated response" systems which some countries have in place against end-users in cases of direct infringement of intellectual property rights (e.g., as envisaged by France's "*Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet* " (HADOPI) Act or Britain's Digital Economy Act).

The reason is that, in such cases, while the ISP has a relevant role in interrupting or blocking the end-user's connection, normally its job is merely instrumental with respect to action against the direct offender, being confined to collaborating with the competent national (judicial or administrative) authority in identifying infringers and disabling service access in the case of repeat infringers.[5]

For this same reason (incidental role of ISPs), no analysis has been made of the conceivable implications of the eventual entry into force of the Anti-Counterfeiting Trade Agreement, (ACTA)[6,7] for some of the signatory countries targeted by this study.

It should be borne in mind, moreover, that this study has focused on infringements suffered by the holders of copyright and related rights, without prejudice to the fact that the conclusions drawn may often be valid where other interests are at a stake, e.g., industrial property rights (trademarks in particular) or even personal rights (good name, privacy, image), a case in which the same enactment is occasionally applied (i.e., the European Union Directive on Electronic Commence); or, that the conclusions reached in cases of copyright infringement may be applicable *mutatis mutandis* to other sectors of the legal system.

At an international level, the specific problem of ISP liability was the subject of intense lobbying at the Diplomatic Conference of the World Intellectual Property Organization (WIPO) in December 1996, which concluded with the adoption of the WIPO Copyright Treaty[8] (WCT) and WIPO Performances and Phonograms Treaty[9] (WPPT).

---

[5] Even so, an Internet intermediary (an access or hosting provider in particular) may sometimes incur liability for not having correctly implemented an injunction for cessation or for not having complied with the detection and removal procedure applicable to the case.

[6] The EU and 22 of its Member States have signed the treaty, though it has not yet been ratified by the European Parliament. Other countries that have also signed the ACTA are Australia, United States, Canada, Japan, South Korea, New Zealand, and, insofar as this study is concerned, Morocco and Singapore.

[7] Section 5 of the ACTA contains a series of rules governing observance of intellectual property rights in the digital environment. Insofar as ISPs are concerned, Article 27.2 states somewhat ambiguously that the procedures for the observance of intellectual property include infringements of copyright and related rights, and that such infringements *could* include the illegal use of means of widespread distribution for infringing purposes. The article goes on to state that the procedures for preventing these widespread infringements must preserve fundamental principles such as freedom of expression, fair process, and privacy, though the footnote to this paragraph adds, confusingly and slightly cryptically, that this can be achieved, for example, *by adopting or maintaining a regime providing for limitations on the liability of, or on the remedies available against, online service providers while preserving the legitimate interests of* [the] *right holder.* For its part, Article 27.4 empowers the legislature of a contracting party to *provide, in accordance with its laws and regulations, its competent authorities with the authority to order an online service provider to disclose expeditiously to a right-holder information sufficient to identify a subscriber whose account was allegedly used for infringement*.

[8] World Intellectual Property Organization Copyright Treaty of 20 December 1996.

[9] World Intellectual Property Organization Performances and Phonograms Treaty of 20 December 1996.

Despite the numerous debates and pressures, agreement could not be reached on including a specific clause in the text of the treaties. Nevertheless, the Agreed Statement concerning Article 8 of the WCT states that, "*It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the Berne Convention. It is further understood that nothing in Article 8 precludes a Contracting Party from applying Article 11bis (2)*"

While this Declaration had the practical value of allaying the doubts of representatives of the telecommunications companies, the limited nature of its scope meant that it did not actually solve the problem. Essentially, therefore, the question of liability of Internet intermediaries must be resolved by having recourse to the respective national laws and the provisions of regional enactments (European Union Law in particular), taking into account the judicial decisions that have applied these.

II. ARGENTINA

1. Legislation

Argentina has no legislation that specifically addresses the civil liability of ISPs,[10] beyond the ratification of the 1996 WIPO Treaties by Act 25.140, which logically includes the implementation of Article 8 of the WCT in Argentine law.

Although there have been a number of parliamentary Bills containing rules on this issue, they have nevertheless failed to find their way onto the statute book. The most recent of these was the Bill of 22 February 2011,[11] tabled by congressman Federico Pinedo, which succeeded two earlier bills proposed by Senators Jorge Capitanich (2006)[12], and Guillermo Jenefes (2009) respectively.[13]

Similarly, there is no specific legislation governing Internet search engines, though it could be argued that, in this regard, Article 10 of Intellectual Property Act 11.723 (governing the so-called "right to quote") or Article 1 of Act 26.032 of 16 June 2005, which expressly provides that, "The *search*, receipt and dissemination of all manner of

[10] Such providers only have the obligation, under Article 1 of Act 25.690 (Official Gazette of 3 January 2003), to offer protection software that bars access to specific sites at the time of offering the Internet services, regardless of whether the service agreement is formalised by telephone or in writing. It appears that what is fundamentally in mind here are access providers, who should thus include parental control software in their service packages.

[11] Bill with dossier number 8793-D-2010, on the regime for Internet service providers, available at website address: http://www1.hcdn.gov.ar/proyxml/expediente.asp?fundamentos=si&numexp=8793-D-2010>. The Bill departed from the principle of subjective attribution of liability to providers for automatic hosting of content generated by third parties *exclusively* in cases where they have effective knowledge that the content housed is illegal or violates third-party rights (Article 2) and, in addition, defines what is to be understood by "Internet service providers", access providers, search engines and hosting providers (Article 1). The Bill also permitted any person to request the competent court for access to be disabled or restricted in respect of content which might prove prejudicial to rights recognised by the Argentine Constitution, international treaties to which Argentina is a party, or Argentine statutes (Article 3 of the Bill). In such as case, the court would, even *inaudita parte*, be able to order the blocking or removal of content, if there were danger of irreparable damage to the rightholder or risk of destruction of evidence. In much the same way as the European Directive, access providers would only be liable, according to Article 5, in a case where they themselves generated the content or where they modified or selected such content or the recipients thereof.

[12] This is Bill S-3812/06, available at the Argentine Senate website address <http://www.senado.gov.ar/web/comisiones/verExpeComi.php?origen=S&tipo=PL&numexp=3812/06&nro_comision=&tConsulta=3>.

[13] The 2009 Bill envisaged the possibility of a person being entitled to require an access or hosting provider to disable access to or block any content in which the name (for natural persons) or corporate name (for legal persons) was included, in any case where such inclusion might "offend said person".

information and ideas via an Internet service is deemed to come within the constitutional guarantee which protects freedom of expression", might be applicable.

In the face of this absence of special legislation, it is but a truism to state that recourse should be had to the general rules of non-contractual liability, though there is a degree of discussion at a doctrinal and case-law level as to whether the criterion of attribution of liability should be objective -based on risk- under Article 1.113, subsection two *in fine* of the Argentine Civil Code, or whether it should instead be subjective -based on *mens rea* or guilt/negligence- under Article 1.109 of the Civil Code.

Based on legal doctrine and judicial decisions handed down to date, it would seem, on balance, that the majority view leans towards the subjective criterion as being the most correct in this case. This requires the Claimant to prove that the intermediary acted with *mens rea* or guilt, either because, on being notified, it failed to remove or disable access to the content matter, or alternatively, because it somehow knew from the outset that the content was unlawful, and is thereby barred from being able to shield itself behind a plea of ignorance or good faith.[14]

2. Case-law

a) *Internet search engines*

The matter of ISP liability for infringement of intellectual property rights has scarcely been broached in the Argentine courts. Even so, there have been a good number of cases (mostly still in the lower courts) in which a series of natural persons (generally well-known personalities, such as artists or professional sportsmen and women) have claimed damages in civil actions against various Internet search engines.

In most of these cases, infringement of personality rights (good name and image) is claimed with respect to the display of search results with hyperlinks that, in turn, direct users to pages on which photographs of the Defendants are shown in relation with pornographic or illegal material.

The most relevant case to date in terms of media impact was that decided by the Buenos Aires Civil Appeal Court's judgement of 11.8.2010, in which the singer of the pop group *Bandana* sued the Argentine subsidiary of *Yahoo* and *Google Inc.,* seeking compensation of 200,000 Argentine pesos by way of moral damages.

The Appeal Court held that the search-engine operator was not liable, reversing the judgement of the Court of First Instance (which had ordered the respective search-engine operators to pay compensation of 50,000 pesos each),[15] on the grounds that the case should basically be decided in accordance with the general rules of non-contractual civil liability (Articles 902 and 1.119 of the Argentine Civil Code), rules that require negligence on the part of the Defendant. The Court held that culpability of this nature could only be deemed to exist in a case where there had been no diligent reaction in response to a possible notification by the Claimant (something that had not occurred in the case in point).[16]

[14] See LIPSZYC, D., "*La responsabilidad de los proveedores de servicios de intermediación en línea*", *Responsabilidad civil y Seguro*, 2009, No. 2, p. 20.
[15] Decision of National Civil Court of First Instance No. 75, of 29 July 2009, available at website address <http://www.hfernandezdelpech.com.ar/JurisprudenciaFalloDaaCunhacYahoo.html>.
[16] The case is currently pending judgement of the appeal brought before the Argentine Supreme Court of Justice.

Aside from this, many more judgements have been handed down by courts of first instance throughout Argentina, with contradictory decisions. For instance, in the case of a model belonging to the *Dotto Models* agency, the Court ordered the search-engine operators sued in the case to pay compensation of 100,000 Argentine pesos,[17] though it made the point that civil liability could not be generated prior to the search-engine operator becoming aware of the wrongful act. In contrast, the decision of the Buenos Aires Lower Civil Court 62 of June 2011 as well as that of the Federal Lower Civil and Commercial Court No. 10 of 26.10.2011 rejected the existence of liability in search-engine operators (both decisions have been appealed).

As can be seen, the question is still open but in the court decisions rendered to date in cases of unlawful invasion of personality rights in Argentina, there is a trend towards the view that only search-engine operators who, on being notified by the aggrieved parties then fail to act diligently to disable access to content, should be deemed negligent. There is also the conviction that, by making use of the analogy, the solution reached in such cases of infringement of personality rights will, in good measure, influence the result in cases where the issue being debated is that of possible copyright infringement by Internet search engines.

b) *Link-listing websites*

With reference to web pages offering hyperlinks, the leading case (and one of the most important in the Spanish-speaking world) is that of Taringa!, in which a number of publishers brought a criminal action for infringement of Article 72 (a)[18] of Intellectual Property Act 11.273. The committal for trial order issued against the accused at the first instance was upheld on 29.4.2011 by Chamber VI of the National Criminal and Correctional Court, which confirmed the involvement of the website administrators as being "aiders and abettors"[19] of the offence committed by the end-users, and likewise endorsed the attachment of assets to a value of 200,000 Argentine pesos (around US $50,000) to provide for any possible liability that might flow from a final sentence.[20]

III. BELGIUM

1. Legislation

a) Directive on Electronic Commerce

Belgium, like the remaining European Union countries which will be mentioned in this study, has had to adapt its national laws governing ISP liability to the regulation

[17] Decision of National Civil Court of First Instance No. 95 of 4 March 2010, *Rodriguez María Belén c/ Google Inc.s /Daños y perjuicios,* available at website address http://www.hfernandezdelpech.com.ar/JurisprudenciaFalloRodriguezcGoogle.html

[18] This provision makes the publication, sale, or reproduction (though not the public communication) of any work without the author's consent, a criminal offence.

[19] It held that, though it might be true that the perpetrators of the deed are those who "upload the work" onto the web page and "download" it, it was no less true that "the convergence of the two was in response to the use of the web page www.taringa.net", which in turn allowed those accused of co-responsibility to be deemed aiders and abettors in the sense of Article 45 of the Argentine Penal Code.

[20] The Court of Appeal's principal argument was that the administrators of the web page clearly knew of the illegality of much of the linked content matter, making efforts that were more apparent than real to control such links.

envisaged by the DEC,[21] an statute that devotes Articles 12 to 15 to clarifying the civil and criminal liability to be faced by ISPs for their commercial activities.[22]
Although this is not the moment to embark upon a detailed explanation of the legal regime under this enactment, a brief reference will nevertheless be made to it, since it fundamentally determines the legal regulation of EU countries, such as Belgium. What is said below about the Directive logically holds true for the rest of the EU countries, though it will not be repeated in each case.

Section IV of the DEC devotes four of its Articles (12 to 15) to setting forth the liability that ISPs must face for their commercial intermediation activities.

The Directive applies to both criminal and civil liability, covering any type of infringement of third-party rights, which includes, among other matters, intellectual and industrial property rights and personality rights (good name, personal and familiar privacy, image, etc.). This is what is known in Community jargon as a "horizontal approach".

As is only logical, in a case where, rather than acting as an intermediary, an ISP acted as a supplier of content (publisher), it would be entitled to avail itself of the limitations of liability envisaged under the Community enactment. Its civil or criminal liability would thus be determined pursuant to the rules in force under the laws of the respective Member States. Similarly, internet service providers (access and storage providers in particular) would be answerable in accordance with their national legislation in any case where they failed to comply with any of the conditions or "safe harbours" stipulated for the different situations.[23]

A further point to be borne in mind is that Articles 12 to 14 of the DEC only afford protection against civil actions for damages, so that actions for injunctions and interim measures invariably remain outside the scope of such protection, as stated in Articles 12.3, 13.2 and 14.3 of the Directive.

Insofar as the legal status of ISPs is concerned, the DEC departs from a basic idea embodied in Article 15.1. This provision exempts service providers from the general obligation to carry out active monitoring or control of online information supplied by third parties. This is a rule of special importance in the case of Belgium, based on the decisions of the Court of Justice of the European Union (CJEU) in the *Scarlet Extended* and *Netlog* cases, which will be discussed in greater detail below.

Premised on this general idea that there is no general obligation to monitor content transmitted or stored in those cases where ISPs undertake intermediation activities, safe harbours can be applied to activities of simple data transmission or provision of access (mere conduit, Article 12 of the DEC), provision of proxy caching (Article 13 of

[21] In its report on the application of Directive 2004/48/CE (COM (2010) 779 final of 22 December 2010), the EU Commission clearly underscored the suitability of entering into a discussion on the possible modification of the regime applicable to persons who collaborate in the online dissemination of protected works and performances (page 6, point 3.1).

[22] The exemptions from liability envisaged by the DEC only apply to intermediary information society providers established in EU countries. For non-community intermediaries, the national rules of liability and Private International Law will apply.

[23] Naturally, the fact that the intermediary may, in the specific case, not comply with the conditions for safe harbours does not automatically determine a presumption of liability. It will be necessary in each case to verify whether the requirements envisaged under the *jus commune* in order for such liability to arise are present, both in the criminal sphere (especially the definition of the conduct as criminal) and in the civil field (especially the relation of causality between the conduct of the intermediary and the damage caused to the third party).

the DEC) and hosting of information supplied by a recipient of the service (Article 14 of the DEC).

With respect to mere conduit activities, Article 12 paragraph one of the Directive exempts intermediaries from liability in cases where they adopt a passive role consisting of transmitting data on behalf of or providing network access services to the recipients of their services (customers or end-users), provided that the ISP has no control over the information transmitted. To verify that the intermediary has no real control over such information, the DEC requires that a series of conditions be met, namely: that the information must be furnished by a third party (thus leaving cases in which the ISP itself makes online material accessible, outside the "safe harbour"); and that the intermediary must neither select the recipients of the transmission nor select or modify the data transmitted.

Article 13 of the DEC is tasked with regulating exemption from liability for system or proxy caching activities, by protecting operators who resort to this mechanism to accelerate the service which they supply to their customers, provided that they fulfil a series of conditions stipulated in the Directive.[24] Despite evincing a certain degree of complexity in its wording, it is a provision which in practice has not posed any significant problems[25] in the European sphere.

With reference to hosting service providers, Article 14.1 a) of the Directive provides that, in any case where an ISP devotes itself to activities of storing information furnished by a recipient of the service, in order for it to be able to benefit from the limitation of liability said ISP must have no "actual knowledge" of the fact that the activity is illegal, or must not be "aware of facts or circumstances from which the illegal activity or information is apparent", i.e., it must not act culpably or negligently in ignoring evident facts that reveal the illegal nature of content matter stored on its servers (*constructive knowledge*).

Article 14 of the DEC thus lays down a dual standard as regards hosting service providers' degree of implication in the activity of end-users. In order for there to be criminal liability, *mens rea* is necessary, i.e., conscious intent to protect, permit or induce the unlawful conduct of end-users, something that entails something more than the mere possibility of becoming aware of such conduct. For a civil action for compensation, however, mere negligent conduct will suffice.

Even in a case where the conditions of Article 14.1 (a) are not met, a hosting service provider may still be entitled to exemption from liability by reason of the principle of diligent reaction under Article 14. 1 (b) of the Directive, provided that it act expeditiously

[24] The first of these refers to the fact that the intermediaries may not modify the information, something that is almost inherent in the technical functioning of *proxy caching*. Secondly, the intermediary must only permit access to cached copies to such recipients as meet the conditions imposed for the purpose by the owner of the cached information, such as the fact that the cached copy may not be used by the end-user to circumvent passwords that protect certain content. Thirdly, the intermediary must comply with rules regarding the updating of the information, specified in a manner widely recognised and used by industry, an ambiguous concept but one which amounts to saying that pages that are automatically or very frequently updated (such as those devoted to stock exchange information or exchange rates) should not be cached. Fourthly, it is essential that intermediary should not interfere in the lawful use of the technology generally accepted and used by the sector for the purpose of obtaining data on the use of the information, a condition which basically seeks to ensure that the caching does not affect pages fitted with a "hit counter" so that access to the cached web page is not tallied on the principal page, with the ensuing loss of income.

[25] Article 13 paragraph one of the DEC defines the characteristics required by reproductions that form part of proxy caching, i.e., that these are to be temporary, provisional, automatic copies made for the sole purpose of enhancing the effectiveness of subsequent transmission of the information to other recipients of the service.

to remove or disable access to the information on somehow obtaining knowledge or becoming aware of the illegal nature of the activity.

At all events, Article 14 paragraph two nevertheless requires that ISPs have no control over end-users, and Article 14.3 stipulates that Member States may require a service provider to terminate or prevent an infringement, or may establish procedures in their national laws governing the removal or disabling of access to information.

These provisions of the Directive have been the subject of various interpretations by the CJEU. Leaving aside the cases of *Scarlet Extended* and *Netlog* (to which I shall refer below on reviewing the situation in Belgium), the CJEU's most relevant decision on this matter to date was undoubtedly that of 12.7.2011[26] (*L'Oreal v. Ebay*). This marked the first time at a European level that the Court had ruled on the degree of civil liability corresponding to a Web 2.0 electronic-commerce platform provider ("operator of an online marketplace" in the words of the judgement) for the sale by its users of products that infringed trademark rights.

In its decision, the Court of Justice held that the safe harbour under Article 14.1 of the DEC may also be applied to the operator of an online marketplace, provided that said operator "has not played an active role allowing it to have knowledge or control of the data stored". In principle, this amounts to vesting *Ebay* with the character of a *passive intermediary*, exempting it from liability for trademark infringements unless evidence can be produced to show that it was cognisant of the illegality of end-users' advertisements.

The Court nevertheless went on to indicate that the operator of an online marketplace must be deemed to play an active role (which thus leaves it outside the scope of the "safe harbour") in any case where "it provides assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting them".[27] Accordingly, the difference between intermediaries that have an active role (active hosting) and those that perform merely passive or automatic tasks has to be decided on a case-by-case basis.

In addition, such an operator had a duty to react, by removing or disabling access to the material, "if it was aware of facts or circumstances on the basis of which a diligent economic operator should have realised that the offers for sale in question were unlawful" or where, "in the event of it being so aware, failed to act expeditiously" (a matter which, in the case in point, must be verified by the court that referred the question for the preliminary ruling concerned).

It is also important to underscore that the CJEU deemed that "actual knowledge" may be acquired, both as a consequence of a investigation undertaken by the operator of an online marketplace on its own initiative, and in the hypothetical case that a third party (e.g. the holder of the infringed trademark rights) should notify it of the existence of the illegal content or information. In this latter case, while it goes without saying that the mere existence of notification does not automatically determine the existence of liability, it is nonetheless one more fact to be borne in mind when it comes to ascertaining whether the operator of an online marketplace really had actual knowledge of such illegality.

---

[26] *L'Oreal S.A. and others v. Ebay International AG and others* (C-324/09), available at website address <http://curia.europa.eu/juris/liste.jsf?language=es&num=C-324/09>.

[27] In the CJEU's view, this active role is not however undertaken in a case where an operator that confines itself to hosting sales offers on its server, determines the conditions on which it is going to provide its service, is remunerated for same, and gives general information to its customers on how to conduct the exchange.

Lastly, the Court stated that the third sentence of Article 11 of Directive 2001/29/CE must be construed as requiring the EU Member States to ensure that the national courts having jurisdiction over the protection of intellectual property rights are empowered to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of the same kind. Such injunctions must be effective, proportionate, dissuasive and not create barriers to legitimate trade.

a) The Act governing certain legal aspects of the information society

The enactment incorporating the DEC into Belgian national law[28] is the Act of 13 March 2003, governing certain legal aspects of information society services.[29]

Article 18 of the Act governs mere conduit activities, establishing a safe harbour in any case where the information is furnished by a third party and the intermediary, neither selects the recipients of the transmission nor selects or modifies the information transmitted.[30]

Article 20 (1) of the Act addresses the question of liability of hosting service providers, establishing a safe harbour in any case where the ISP does not have actual knowledge of the illegal activity or information and, with respect to civil claims for damages, is not aware of any facts or circumstances from which the illegal activity or information is apparent (*constructive knowledge*).

Article 20 (1) subsection two also establishes the existence of an exemption from liability for any service provider who, upon obtaining such knowledge or awareness of the illegal nature of content matter stored, acts expeditiously to remove or disable access to such information. To perform this task of removal or disablement, the ISP must use the procedure envisaged under Article 20 §3, which provides for notification to the Public Prosecutor's Office pursuant to Article 39 of the Criminal Procedure Code. Until such a time as the Public Prosecutor should take a decision in this regard, the hosting service provider must restrict itself to disabling access to the material, without deleting it entirely.

Lastly, Article 21 of the Act establishes the absence of a general monitoring obligation, in line with Article 15 of the DEC. Hence, Article 21 (1) paragraph one lays down that ISPs who carry out the activities mentioned in Articles 18, 19 and 20 are under no obligation to monitor the information which they transmit or store, or actively to seek facts or circumstances indicating possible illegal activities by the recipients of their services.

This absence of a general monitoring duty does not however bar the competent judicial authority from ordering temporary monitoring for a specific case (Article 21 (1)

[28] There have also been some unsuccessful Bills that have sought to introduce a "graduated response" system which requires the collaboration of ISPs to identify the users and the issue of network disconnection warnings. This is the case of the so-called "Clarinval Act ", proposed on 26 January 2011 by Senators Clarinval, Ducarme, Jardin and De Donnea Perman, and available at website address <http://www.lachambre.be/FLWB/PDF/53/1120/53K1120001.pdf>. Article 5 of this Bill required access providers to include references in their end-user agreements to intellectual property rights and to the negative consequences which infringement of rights has in terms of employment and cultural diversity.

[29] *Moniteur Belge/Belgisch Staatsblad* of 17 March 2003. The Act is available at website address <http://www.ejustice.just.fgov.be>.

[30] Paragraph two, along the lines of Article 12.2 of the Directive, establishes an exemption from liability for providers who make transient copies of the information that they transmit.

paragraph two), provided that this is envisaged by statute. There is, in addition, an obligation to collaborate with and inform the competent judicial/administrative authorities (Article 21 (2) subsection one, as amended by Article 59 of the Act of 20 July 2005). In this case, the intermediary is bound to communicate any information available as a soon it becomes aware of illegal activities undertaken by the recipient of its services (Article 21 (2) subsection two). There is also a duty to furnish all relevant information relating to any online infringement committed by the end-user, at the request of the competent judicial or administrative authority.

2. Case-law

a) *ISP liability*

As noted above, the CJEU's decision of 24.11.2011[31] in the *Scarlet Extended* case was particularly important in Belgium. A civil action was brought against an Internet service provider (*Scarlet*) by the Belgian rights management society, *Société belge des auteurs, compositeurs et éditeurs SCRL* (SABAM), seeking the implementation of a filtering system that would prevent ISP customers from exchanging files over P2P networks pursuant to Article 87 (1) of the Copyright Act.[32]

The Court of First Instance ordered the ISP to put a halt to the infringement by installing a filtering system that would prevent files from being exchanged by end-users but *Scarlet* appealed against the decision, claiming that such filtering amounted to a general monitoring obligation in breach of Article 15 of the DEC, thus leading to the Brussels Court of Appeal's decision to refer the question to the CJEU for a preliminary ruling.

In its decision, the CJEU ruled that the filtering system proposed by the Court of First Instance entailed carrying out a task of controlling traffic to ascertain both the total number of files exchanged by end-users and which of these were unlawful, something that in practice implied the establishment of a general monitoring obligation vetoed by Article 15.1 of the DEC.[33]

b) *Web 2.0 intermediation activities*

The Brussels Commercial Court's decision of 31.7.2008[34] (*Lancome v. Ebay)* held that the electronic auction platform operator against which the action was brought was to be deemed a hosting service provider for the purposes of Article 14 of the DEC, and could

---

[31] *Scarlet Extended S.A. v. Societé belge des auteurs, compositeurs et éditeurs SCRL* (SABAM), case C-70/10, available at the CJEU's main website address <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-70/10>.

[32] The Belgian Act is available from WIPOLex at website address <http://www.wipo.int/wipolex/es/text.jsp?file_id=125255>.

[33] The Court also deemed that this would run counter to Article 3 of Directive 2004/48 (hereinafter referred to as the Anti-piracy Directive), which prohibits the adoption by Member States of measures to protect intellectual property rights that would be excessively complicated or costly, not fair and equitable, or disproportionate. It also drew attention to the principle of balance of rights, laid down by the CJEU's decision in the *Promusicae* case (judgement of 29 January 2008-C-275/26), stating here that, to establish an obligation to filter all online content subject to no time limit would amount to a violation of the principle of freedom of enterprise vis-à-vis the access provider, which is a fundamental right guaranteed by Article 16 of the Charter of Fundamental Rights of the European Union. The CJEU further held that the obligation to order the filtering of content would not guarantee a fair balance between the protection of intellectual property rights and the rights of *Scarlet*'s customers, specifically their fundamental right to the protection of personal data under Article 8 of the Charter (due to the handling of the IP addresses used for the exchange of files) and their freedom to receive or communicate information under Article 11 of the Charter (because the filtering system could not correctly differentiate between content that was lawful and unlawful).

[34] The decision is available at website address <http://www.loeb.com/files/>.

thus benefit from the safe harbours envisaged by the Directive and from the absence of a general obligation to monitor the material auctioned by the site's users.

Furthermore, as indicated above, the CJEU's decision of 16.2.2012 in the *Netlog* case is of special importance in Belgium.[35] In this case, SABAM requested that the social network, *Netlog*, implement a system for filtering content housed on its platform, in order to prevent users from offering files containing copyright-protected literary or artistic works via their online profile.

The court held that *Netlog* answered to the definition of a "data-hosting service provider" under Article 14 of the DEC, and that to establish a general obligation to filter content in this social network would be incompatible with the absence of a general content-monitoring obligation under Article 15.1 of the DEC.[36]

c) *Link-listing websites*

With respect to web pages that act as a repository for or databases of hyperlinks which convey the user to content that infringes intellectual property rights, the leading example in Belgium is the Antwerp Court of Appeal's decision of 26.9.11 in the *The Pirate Bay* case.[37]

The Court stated that the Claimants' plea to have access disabled, in order to prevent Belgian end-users from being able to gain entry to said hyperlink portal, was compatible with the exemption from liability envisaged under Article 12 of the DEC. In addition, it held that any disabling measure had to be technically possible, proportionate and entail a reasonable cost.

d) *Internet search engines*

In the case of *Google v. Copiepresse et al.,* the Brussels Court of Appeal's judgement of 5.5.2011[38] decided the action which brought the Belgian newspaper copyright management company (Copiepresse) into confrontation with different Google services, though in only one of these (*Google News*) did the Court really address the issue of whether the search-engine operator was carrying out genuine intermediation activities[39] or whether the case before it was one of direct infringement.

With respect to said service, the Court concluded that, in line with the CJEU's decision in the *Infopaq* case,[40] the reproduction of the headlines and initial lines of the

---

[35] *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (Sabam) v. Netlog NV,* (C-360/10), available at <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-360/10>.

[36] The doctrine in the *Scarlet Extended* case was also repeated on the CJEU stating that this filtering activity would also run counter to Article 3 of the Anti-piracy Directive, and that it would infringe the hosting provider's right of freedom of enterprise, as well as its right to protection of personal data and freedom to send and receive communications.

[37] *VZW BAF v. Belgacom and Telenet,* available at <http://www.edri.org/files/piratebay-decision-belgium-2011.pdf>.

[38] The decision is available at <http://static.ow.ly/docs/Copiepresse5mai2011_eM3.pdf>.

[39] This is because the first of the activities to which the decision refers, that of the search engine operator's cache memory, is not an intermediation activity. It is the search engine robot itself which reproduces the content and subsequently communicates it to the public. Hence, as the Court of Appeal stated, the consent of the copyright holders is needed to authorise such acts of reproduction and communication to the public.

[40] See the CJEU's decision of 16 July 2009 (Case C-5/08 *Infopaq*), which held that the reproduction, storage in digital memory and print-out of an excerpt comprising eleven consecutive words constituted a *partial reproduction* for the purposes of Article 2 of the DDASI *if the product of said procedure is the expression of the author's own intellectual creation* (an aspect that can only be verified by the court of the Member State that referred the question for a preliminary ruling to the CJEU).

newspaper articles in the results yielded by the search engine amounted to an act of partial reproduction of said articles, which should generate some form of remuneration for the authors, inasmuch as the exception for quotations was not applicable in this case.[41]

As regards the applicability of the privileged status afforded to the *Google News* service by the DEC, the Court held[42] that the search-engine operator could not benefit from the safe harbour envisaged for hosting service providers under the Belgian Act because, rather than being limited to having a merely passive role in the storage of information, its activity extended to organising and modifying content when it came to drawing up the news summaries.

IV. BRAZIL

1. Legislation

Currently, Brazil possesses no legislation that specifically addresses the issue of ISP liability. It should also be borne in mind that neither has this country taken steps to ratify the 1996 WIPO Treaties, which logically implies that Article 8 of the WCT is not applicable in Brazilian law.

The country is however witnessing the passage of Bill[43] No. 2.126 of 2011, which seeks to put in place "principles, guarantees, rights and duties for Internet use in Brazil,"[44] a proposed enactment that would introduce into Brazilian legislation the obligation of storing and preserving end-user connection data (Articles 10 and 11 and 12), an obligation that has never been imposed on Brazilian intermediaries until now.

As regards ISP liability for rights infringements committed by recipients of their services (with respect to both intellectual property and other legally protected rights), Article 14 of the Bill establishes a general exemption from liability for access providers ("Internet connection provider", in the terminology of the Act), without making this exemption subject to any other additional requirement or condition.

For its part, Article 15 of the Bill lays down that, save where otherwise provided, an "Internet applications provider" may not be held liable for damage caused by content matter generated by third parties, except in a case where, following a specific court order, it fails to take the appropriate measures, within the scope of its services and the time limit indicated in the writ of court, to disable access to content defined by the court as infringing. Said liability is not subject to any other additional requirement or condition.

---

[41] The Court additionally concluded (in sharp contrast with the German Supreme Court's decision of 29.4.2010 in the case of the *Google Images* service, to which reference will be made below) that there was no room to speak of an implicit licence, due to the fact that the newspapers had not used technical mechanisms to prevent the copying by their robots which searched for data on the Internet, since the right of reproduction belongs exclusively to the authors, who may not be deprived of it by the mere fact of having omitted a technical dossier.

[42] The Brussels Court of Appeal also concluded that the temporary copies made by the search engine operator on its servers did not come within the definition of system caching under Article 13 of the Directive because, rather than seeking to accelerate online transmission, it sought instead to store a copy of the websites consulted.

[43] There was a prior bill, dating from 2005 (Bill 84/99) and known as the "Azeredo Act", named after the senator who tabled it, which gave rise to controversy in the mass media and was ultimately withdrawn.

[44] PL 2126/2011, information on the Bill's passage and text is available at website address <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255>. This Bill arose from a process of debate open to public consultation in 2009, aimed at drawing up a general law in the field of Internet legislation (known as the "civil framework" of Internet), and, with regard to possible ISP liability, regulating matters such as user rights (Article 7), principle of online neutrality (Article 9), etc.

The provision is somewhat unclear but, given that "Internet applications" are very generally defined by Article 5.VII of the Bill as "any set of functionalities accessible via a terminal connected to the Internet", the reference to an "Internet applications provider" would seem to extend to different cases, such as those of hosting service providers, ISPs engaging in proxy caching activities and even the activity of online search engines, which would thus be subject to this special liability regime, one that can solely arise on receipt of a duly certified court order.[45] Only in the event of direct disobedience of such a court order could the ISP become liable.

The Bill moreover requires the intermediary to notify the end-user that it has proceeded to remove or disable the content, provided that the ISP has sufficient data to serve such notice (Article 16 of the Bill), and establishes the procedure and requirements for the parties to seek a civil or criminal court order for delivery of the data by the intermediaries in any case of illegal activities undertaken by the users of their services (Articles 18 and 19).

Parallel to this ISP Liability Bill, a reform has been proposed for adapting copyright to the digital environment (fundamentally with respect to limits and exceptions to ownership rights),[46] which would include a new wording of Article 105 of the Copyright Act No. 9.610 of 19 February 1998. The proposed wording would permit the competent court to act directly, by ordering the removal or blocking of any material issued or made available on the Internet which involved infringement of the intellectual property rights of its holders, and provides for a penalty of a daily fine to be levied on any ISP that failed to comply with such an order, without prejudice to any other compensation or criminal penalties that might exist. The rule moreover envisages the doubling of the fine in the event of there being evidence to show that the infringer is a repeat offender.

At all events, until the above-mentioned regulation in both Bills sees the light of day (if that indeed should finally occur), the matter of ISP liability must be resolved in the civil courts by application of the general principle of culpable liability under Article 927 of the Civil Code[47] or, alternatively, by having recourse to the special rule contained in Article 104 of the 1998 Copyright Act 9.610,[48] which lays down the principle of joint and several liability with respect to the principal infringer and all those who market the infringing merchandise for gain.[49] It seems that this rule could be applied by analogy to ISPs in the case of online infringements, at least insofar as civil actions are concerned.

In criminal matters, Article 12 of the Computer Programme Protection Act 9.609/98 of 19 February[50] and Article 184 of the Penal Code[51] (in the wording of Act 10.695 of 2003) apply to infringements committed in respect of other types of literary and artistic works enjoying copyright protection. Both provisions draw a distinction between infringement for commercial and non-commercial purposes, with the latter case

[45] To this end, the sole paragraph of Article 15 lays down that the order must, on pain of being rendered null and void, contain clear and specific identification of the content infringer, so as to enable unequivocal location of the material.
[46] The consolidated version of the Act, with all the proposed amendments, is available on the Ministry of Culture's web page, at <http://www.cultura.gov.br/consultadireitoautoral/wp-content/uploads/2010/06/Lei9610_Consolidada_Consulta_Publica.pdf>.
[47] Approved by Act No. 10.406 of 10 January 2002, available at website address <http://www.wipo.int/wipolex/es/text.jsp?file_id=226198>.
[48] The 1998 Act is available at <http://www.wipo.int/wipolex/es/details.jsp?id=514>.
[49] The law holds as being jointly and severally liable any persons who sell, exhibit for sale, conceal, acquire, distribute, store or use a fraudulently produced work or phonogram, for the purpose of selling, obtaining a direct or indirect profit, advantage, benefit or gain, for themselves or a third party.
[50] The Act is available at website address, <http://www.wipo.int/wipolex/es/details.jsp?id=513>.
[51] The Brazilian Penal Code was originally approved by Legislative Decree No. 2.848 of 7 December 1940, and is available at <http://www.oas.org/juridico/mla/pt/bra/pt_bra-int-text-cp.pdf>.

carrying a lighter penalty.[52] In the case of intermediation conduct involving coincidental contribution to the wrongful act, the general rules of co-responsibility will be applied where there are two or more offenders (Article 29 of the Penal Code).

2. Case-law

In view of the doubts posed by application of the general rules to this particular case, the matter of ISP's civil liability for copyright infringement has still to be directly resolved by the Brazilian courts,.

In civil case-law, until now the role of ISPs has been limited mostly to being the recipients of requests to reveal the identity concealed by an IP address from which files are exchanged over P2P networks, as occurred with a barrage of some 20 actions brought by the Brazilian Association of Record Producers (*Associação Brasileira dos Produtores de Discos - ABPD*) in 2006[53] against different end-users (most of whom were located in the city of Sao Paulo).

The actions were unsuccessful, however, because at the time ISPs had no obligation under Brazilian law to preserve the connection data of their end-users, which in turn rendered it impossible for such users to be reliably identified[54] (as noted above, one of the main designated aims of Bill No. 2.126 of 2011 was to close this loophole in Brazilian law).

There is nevertheless consolidated case-law in the Brazilian High Court of Justice (*Superior Tribunal de Justiça*), the highest judicial body in the land, in cases of infringement of personality rights in social networks, which could be applied, *mutatis mutandi*, to cases of copyright infringement on Web 2.0 intermediation platforms.

The leading example is to be found in the decision of 14.12.2010,[55] in a case of infringement of the right to a good name in the social network, *Orkut* (operated by *Google*), in which the Court held that a social network operator cannot be found liable for offensive content posted by end-users, nor can it incur objective liability envisaged under Article 927 of the Brazilian Civil Code.

Notwithstanding this, however, as soon as a social network operator becomes aware of the illegal nature of the content, it must act *vigorously* to remove such content from the network or disable access to it immediately, under pain of being held jointly and severally liable along with the party directly responsible for the damage.[56]

---

[52] In the case of software activity, the offence is only prosecuted at the instance of the party, both where the infringement is committed for commercial purposes and in any other case. In the case of the Penal Code, the offence is prosecuted at the instance of the Department of Public Prosecutions where the infringement is for commercial purposes, and is otherwise subject to a complaint being lodged by the aggrieved party.

[53] See the summary of these cases in MIZUKAMI, P., CASTRO, O., MONCAU, L.F. and LEMOS, R., "Capítulo 5. Brazil" in *Piratería de Medios en las Economías Emergentes,* Social Science Research Council, pp. 246-247, e-version available in PDF format at website address <http://piracy.ssrc.org/wp-content/uploads/2012/04/MPEE-ESP.pdf>.

[54] One of the judges tasked with deciding the case refused to request data from the ISPs, whereas in another case a request was made to the ISPs, who pleaded that they had already deleted the data on being under no obligation to retain same pursuant to the Brazilian legislation then in force. See this explanation in MIZUKAMI, P., CASTRO, O., MONCAU, L.F. and LEMOS, R., "Capítulo 5. Brazil" in *Piratería de Medios en las Economías Emergentes,* cit., p. 281.

[55] Special Appeal No 1.193.764, *IP DA SB v. Google Brazil Internet LTDA,* available at website address <https://ww2.stj.jus.br/>.

[56] In addition, there is the obligation to reveal the identity of the author of the comments through the record of the IP address employed by the user.

This doctrinal idea is reiterated in almost identical terms in at least three subsequent decisions of this same Court, dated 9.8.2011,[57] 23.8.2011[58] and 13.4.2012,[59] which moreover clarify the fact that a social network has no *a priori* duty of filtering or monitoring material.

It would therefore seem that, in the event of infringements of personality rights committed by end-users, Brazilian case-law lays down a principle of limitation of liability for Web 2.0 platform operators while such operators have no actual knowledge of the infringement, a doctrine that may doubtless also be applied by analogy to the case of infringement of intellectual property rights.

In addition, there are some informal agreements between the holders of copyright and related rights and some ISPs who have, *de facto*, adopted a notice and take down process with respect to content, which has led to many websites voluntarily complying with notifications from owners in any case where the latter detect intellectual property right infringements,[60] thereby avoiding the need to have recourse to the law courts.

V. CHILE

1. Legislation

Regulation of the issue of ISP liability in Chile has been influenced by the signing of the Free-Trade Agreement (FTA)[61] between Chile and the United States on 6 June 2003,[62] which forced Chilean lawmakers to adopt rules, clearly inspired by the provisions of the US DMCA and designed to exempt internet service providers from liability.

Indeed, Chapter 17.11.23 of the FTA establishes an ISP liability regime that calls upon Chilean lawmakers to adopt limitations of liability for activities of mere data transmission (transmitting, routing or providing Internet connections),[63] proxy caching (caching carried out through an automatic process*)*,[64] provision of hosting[65] and, lastly, referring or linking users to an online location by using information location tools, including hyperlinks and directories,[66] as well as rules governing notice and take down of content.[67]

For the purpose of incorporating this FTA provision into the country's internal law, Act 20.435 of 4 May 2010 was passed,[68] amending Intellectual Property Act 17.236 and so making Chile the first country in South America to have this type of regulation.

---

[57] Special Appeal No. 1.1175.675, *Google Brazil Internet Ltda v. Tiago Valenti*. The decision is available at website address <https://ww2.stj.jus.br>.
[58] Special Appeal No. 1.186.616, *Google Brazil Internet LTDA v. Alexandre Magno* Silva *Marangon,* available at website address <https://ww2.stj.jus.br/>.
[59] Special Appeal No. 1.306.066, *Google Brazil Internet LTDA v. Mauro Sergio Pereira de Assis*, available at website address <https://ww2.stj.jus.br/>.
[60] According to MIZUKAMI, P., CASTRO, O., MONCAU, L.F. and LEMOS, R., "Capítulo 5. Brazil" in *Piratería de Medios en las Economías Emergentes,* p. 281, though I was unable to gain access to these agreements.
[61] Chile also forms part of the negotiations of the Trans-Pacific Partnership (TPP) Agreement, the latest known draft of which contained a regulation governing ISP liability (Article 16).
[62] Published in the Official Gazette of 30 December 2003. The Agreement is available at website address <http://www.prochile.cl/tlc/chile_usa/compras_publicas/texto_acuerdo.pdf>.
[63] Section 23, subsection b) i) of the Agreement.
[64] Section 23 subsection b) i) ii) of the Agreement, subject to compliance with the conditions laid down in subsection c).
[65] Section 23, subsection b) i) iii) of the Agreement.
[66] Section 23, subsection b) i) iv) of the Agreement.
[67] Section 23, subsections d), e), f) and g) of the Agreement.
[68] The Act is available at website address <http://www.leychile.cl/Navegar?idNorma=1012827>.

This Act adds subsection y) to Article 5 of the Intellectual Property Act, defining a "service provider" as any company that supplies services of transmission, routing or connections for material without modification of its content, furnishes physical facilities, or provides access.

Furthermore, under Title III, the Act adds a new Chapter III. Its pivotal provision is Article 85 I, which establishes a general limitation of liability for ISPs without prejudice to that which might correspond to recipients of their services under the general rules.[69] Where the conditions stipulated in each case by the Act are fulfilled, intermediaries will not be required to pay compensation for damage caused, and are only subject to preliminary and judicial actions for injunction mentioned in Article 85 R.

Article 85 M governs the exemption from liability for providers of transmission, routing or supply of Internet connections,[70] laying down that such parties shall not be liable for the data transmitted if they comply with given conditions of neutrality (i.e., not selecting or modifying the information contained in the transmission, not initiating the transmission, and not selecting the receiver of the transmission).[71]

Article 85 N regulates the safe harbour for providers of caching carried out through an automatic process (proxy caching), who are not to be deemed liable for the information stored provided that they abide by the conditions stipulated by the Act, which are very similar to those to be found in other statutory enactments.[72] It likewise establishes a principle of diligent reaction in the matter, by requiring the intermediary -Article 85 N d)- to act expeditiously to remove or disable access to the material where it has been deleted from the website of origin, provided that notification of said removal has been given to the ISP by means of the procedure envisaged under Article 85 Q.

Article 85 Ñ regulates the exemption from liability for hosting service providers, including as such those who provide search and reference services by means of online hyperlinks (search engines). The conditions established for benefiting from the exemption from liability are basically two: firstly, the provider must have no actual knowledge of the illegal nature of the data; and secondly, it must receive no financial benefit directly attributable to the infringing activity.

Furthermore, in any case where an ISP has the right and ability to control such activity, for it to be eligible to benefit from the safe harbour it must, not only publicly designate a representative tasked with receiving the judicial notifications that declare the content to illegal, but must also react with diligence by expeditiously removing or disabling access to the material stored, on obtaining actual knowledge of its illegality.

Actual knowledge is *only* acquired where there is a judicial decision that orders the removal of or disabling of access to the data, notice of said judgement has been duly served under Article 85 Q, and the order has been ignored or disobeyed by the ISP.

---

[69] When Article 85 L refers to the fact that the exemptions from civil liability apply "without prejudice to the general rules governing civil liability", I take this to be referring to the liability of users because, insofar as ISPs are concerned, it must be understood that Act 20.435 is special legislation *ratione materiae*.

[70] The Act does not directly refer to the activity of "provision of access" but rather to "provision of connections", unlike the FTA in which network access activity is clearly mentioned.

[71] The limitation also extends to acts of transient storage in the process of digital transmission over the Internet, in much the same way as occurs with Article 12.2 of the DEC.

[72] They are required to comply with conditions on access to the information and rules regarding the updating of the information specified by the original website provider, not to interfere with the lawful use of technology used by the website provider to obtain information about the online use of the stored content, and not to modify the information.

A mere complaint or notification by the rightholders affected will not therefore suffice, nor is the intervention of an administrative body envisaged: the entire process takes place in the courts.

Article 85 O of the Act lays down a group of common conditions applicable to all intermediation activities mentioned in Articles 85 M, N and Ñ. These require that intermediaries make public the general conditions applicable to the service provision contracts with their end-users, specifying how said contracts are to be terminated in any case where end-users are judicially defined as repeat infringers of intellectual property rights.

Further requirements are that intermediaries must not interfere in the use of effective technological protection measures and digital copyright information systems (which are envisaged under the FTA with the United States and are also incorporated into the Intellectual Property Act by Act 20.435), and that the ISP must neither generate the content nor select the recipients thereof (with the exception, in this latter case, of Internet search engines).

In the case of Chile, Article 85 P establishes the absence of a general obligation for providers to monitor the material exchanged by end-users of their services, as well as the absence of any obligation to conduct active searches for facts or circumstances that might indicate illegal activities, without prejudice to any *ad hoc* investigation activities that the law courts might implement for this purpose.

Article 85 Q is the provision which sets out the process for notice and take down of illegal content with judicial intervention. This procedure enables the rightholder to seek an interim (preliminary) or final injunction as envisaged under Article 85 R.[73] In order for the plea submitted to the court to have validity, a series of conditions stipulated in Article 85 Q paragraph two must be verified (clear identification of the infringed rights, owners, infringing material, etc.).

Once this plea has been entered, the court must forthwith order the disablement or removal of content alleged to be unlawful, though the end-user affected (the *publisher* or supplier of content) shall be entitled to request the court to set aside the disablement or removal order, pleading all such facts or circumstances as it deem fit in the pertinent counter-notification.[74] In this same procedure, the civil court can order the ISP to furnish all such data as might enable the publisher to be identified (Article 85 S), and can likewise order the closure of the accounts of repeat infringers, provided that these are correctly identified and that the service has been used to carry out activities of infringement of copyright or related rights.

In all the above cases, the court issuing the injunction must take into account the burden or encumbrance that this would entail for both the ISP and the customer, the damage to the intellectual property rightholder, the technical feasibility and effectiveness of the measure, and the existence or absence of other less burdensome ways of ensuring respect for the right in question.

To conclude, Article 85 T of the Act provides that any party who wilfully furnishes false information about alleged rights infringements must pay compensation for the damage

[73] In the case of the interim procedure, the measure may be adopted, even *inaudita parte*, by the civil court if there are pressing reasons that render this advisable, on condition that the Claimant lodge the necessary security, without prejudice in every case to any possible criminal actions that might be brought.

[74] In addition, Article 85 R lays down that court orders directed at intermediaries who carry out mere conduit activities (transmission, routing or provision) aimed at blocking access to given infringing content shall in no way mean that access may be barred to other lawful content.

caused, and Article 85 O provides that the complete notification made by the rightholder pursuant to Article 85 Q must be communicated to the alleged infringer.

The point should also be made here that, at a legislative level, Act 20.453[75] added some new articles to the General Telecommunications Act 18.168, for the purpose of enshrining the principle of online neutrality for Internet consumers and end-users,[76] by requiring ISPs not to intervene in content.

2. Case-law

The problem of ISP liability was posed much earlier in Chile than in other countries on the subcontinent, on the occasion of the *Recurso de Protección. Orlando Fuentes Siade vs. Entel SA* case,[77] decided by the Concepción Court of Appeal on 6 December 1999.[78]

In this case, a citizen filed a claim against the National Chilean Telecommunications Company because an advertisement had appeared on its website, offering the sexual services of the aggrieved party's daughter (who was below the legal age of majority at the time), which led to receipt of a spate of lascivious calls that eventually led to the Claimant having to request that his telephone be disconnected.

In response to the plea for compensation for the damage suffered, *Entel* claimed that the advertisement in question had been placed online by one of its end-users, and that the company's role in this case was simply to function as an electronic notice board, in respect of which it was the end-users themselves who were to be held liable for any content that they advertised.

The Court of Appeal held that the rules of General Telecommunications Act 18.168 were inapplicable to access and hosting providers, stating that in such cases, the issue of liability should be tried by reference to general civil and criminal rules (it should be noted here that the case was decided more than 10 years before the introduction of exemptions from liability under Act 20.435).

To this end, the Court drew a distinction between the different actors involved, establishing liability with respect to both the publisher (in this case, the end-user who placed the advertisement) and to the network access and hosting service providers (in both cases, ENTEL). The Court concluded that the ISP was exempt from liability, in

[75] The Act is available at website address <http://www.leychile.cl/Navegar?idNorma=1016570&buscar=Act+20453>.

[76] The most relevant for the purposes of this study is Article 24 H, subsection a), which requires access providers not to intervene in any way in the exchange of content undertaken by the users of their services, though this is stated to apply to any *legal* activity engaged in or use made by such users. It further requires said providers to make no arbitrary distinction as between content, applications or services based on their source, origin or ownership, and authorises them to take technical online traffic management measures (paragraph three). Article 34 H, subsections b) and c) require access providers to furnish, at users' expense, content-blocking services at the request of the users themselves (in a case where, for instance, parental control systems are used to restrict browsing among minors).

[77] Santiago Schuster Vergara states that said decision was "the first handed down in Latin America", and that it had great influence on subsequent debates about the issue. See SCHUSTER VERGARA, S., *Responsabilidad en las redes digitales y responsabilidad de los prestadores de servicios de intermediación en línea*, available at <https://www.u-cursos.cl/derecho/2009/2/D127C0516/2/material_docente>.

[78] Rol 243-19-99. The text of the decision will be found available at website address <https://www.ucursos.cl/derecho/2008/0/DIPDERINFO/1/material_docente/previsualizar?id_material=177500>.

view of the fact that the advertisement was partly deleted by the company in August 1999 on obtaining knowledge of its illegal nature.[79]

The Court further held that ENTEL had to assume the obligation of adopting the necessary measures to prevent any other advertisements that might be in breach of the Act, morals or public policy from being published on the web page in future, a monitoring obligation which, however, is now expressly rejected by Article 85 P of Act 20.425.

This case had a second episode, corresponding to a civil claim which, rather than seeking the protection of the aggrieved party's fundamental rights (subject of the law suit settled in 1999), sought compensation for the damages suffered at the hands of both the ISP and the person from whose computer the advertisement had been uploaded onto the Internet. Insofar as the ISP was concerned, this claim was also dismissed by the decision of the Concepción Court of Appeal of 21.12.2007,[80] on the ground that at no time had it been in breach of its duty of supervision or care, since it had initially been ignorant of the infringement and had reacted diligently as soon as it became aware of said illegality.

As regards case-law application of the reform introduced by Act 20.425, it would appear that no specific court decisions have yet been handed down.[81]

VI. FINLAND

1. Legislation

a) *ISP liability: Act 458/2002*

Finland has been affected by the regulation of ISP liability by the Directive on Electronic Commerce, implemented in the national legislation by the Provision of Information Society Services Act 458/2002.[82]

This Act, closely following the Directive, firstly contains an exemption from liability for providers of mere transmission and access (mere conduit) services, who are not to be held liable for content in any case where they do not initiate the transmission, do not select the receiver of the transmission, and do not select or modify the information contained in the transmission (Article 13 of the Act).

The exemption for providers of proxy caching services is to be found at Article 14, whose thrust is very similar to that of the DEC,[83] and the exemption for hosting providers is to be found at Article 15, in which the application of the safe harbour depends on the fact that the hosting service provider does not act at the request of the

[79] The Court nevertheless found *obiter dicta* that it would indeed be fitting for liability to be attributed to ENEL as the creator of a database (an electronic platform) fed by contributions from customers, if the minimal measures of care were not taken to identify said customers or where there was knowledge of the unlawful nature of the content and it then failed to act with due diligence to remove said content or disable access to it. Its inactivity in this case thus became culpable or negligent, which led to the possibility of liability being attributed to it by reason of co-operation in the user's unlawful activity.

[80] *Paulina Fuentes Almendra y otro v. Entel, S.A.y otro*, Rol 1223-2003.

[81] News of this is given by ÁLVAREZ VALENZUELA, D., "*En busca de Equilibrios Regulatorios: Chile y las recientes reformas del derecho de autor*", available at <http://ictsd.org/downloads/2011/12/en-busca-de-equilibrios-regulatorios-chile-y-las-recientes-reformas-al-derecho-de-autor.pdf>.

[82] An English translation of said Act is available at <http://www.finlex.fi/fi/laki/kaannokset/2002/en20020458.pdf>.

[83] The usual conditions are included in these cases, in line with the DEC, namely, that the information is not to be modified, that the updating rules prevailing in the sector are to be observed, etc.

party housing the material but reacts expeditiously by removing or disabling access to such material upon the ISP obtaining actual knowledge of the illegality of the information stored through a court order (Article 15.1, subsection one).[84] The specific procedure for removing or blocking illegal information at the instance of the court or Public Prosecutor's Office is detailed in Article 16 of the Act.

Furthermore, a singularity of the Finnish regulation vis-à-vis other EU countries is that actual knowledge of the illegality of material housed may also be obtained by notification on the part of the intellectual property rightholders (Article 15 1) subsection two), provided that said notification by such private parties is effected in accordance with the requirements and conditions stipulated in Articles 20 to 25 of the Act (notice and take down process), which applies in the specific case where the content housed infringes copyright and related rights (but not in the case of infringement of other legally protected rights).

This procedure is initiated by a well-founded request to the ISP by the holders of copyright or related rights (Article 20.1 of the Act),[85] a request which must be sent to the contact that address hosting service providers are compulsorily required to furnish for such purposes. The specific procedure for giving notification is outlined in Article 22 of the Act, a provision that requires said notification to have a minimum content, which is essential for it to be valid.[86]

Upon receipt of the private party's complaint, the ISP must advise the supplier of the allegedly unlawful content of the existence of said notification, the validity of which may be challenged by the publisher within a period of 14 days by means of a "counter-notification", wherein it sets forth the reasons that render the request for withdrawal groundless (Article 23 of the Act).

Should the ISP receive said counter-notification within the designated time limit, it cannot automatically proceed to remove or block the content matter but must wait until agreement is reached between the rightholders and the end-user affected or until there is a judicial or administrative decision on the matter (Article 24).

To conclude this explanation of the Finnish Act, mention should be made of the fact that the provision of Article 15 of the DEC covering the absence of a content-monitoring obligation has not been expressly incorporated in this country, undoubtedly because, as in the case of other EU countries (Denmark, Holland, Spain), said obligation has been construed as not existing in a general manner for any intermediary, including, by extension, ISPs.[87]

---

[84] There is also an obligation to remove housed content in any case where, by any means, effective knowledge (actual knowledge) is obtained that said housed content is "clearly contrary" to Articles 8 of Chapter 11 and 18 of Chapter 17 of the Penal Code (criminal offences of inciting ethnic unrest and dissemination of obscene or pornographic content, respectively), as envisaged under Article 15.2 of Act 458/2002.

[85] The notification must initially be directly addressed to the supplier of content (publisher), though, if said supplier cannot be identified or if the content is not immediately removed voluntarily, it may be directly addressed to the intermediary following the procedure envisaged under Article 22 (Article 20.2 of the Act).

[86] This minimal content includes a list or inventory of the files or allegedly illegal content, a sincere declaration that said content, in the opinion of the party sending the notification, is illegal, evidence that the rightholder has tried in vain to contact the supplier of the allegedly illegal content or that he/she has been unable to identify said supplier, and evidence or a certificate testifying to the ownership of the housed content. Wilful provision of false or inaccurate information places rightholders under an obligation to pay compensation for any damage so caused (Article 25 of the Act).

[87] See in this regard VV.AA., "Study on the Liability of Internet Intermediaries: National Report Finland", 2007, available from the web page of the European Commission at <http://ec.europa.eu/internal_market/ecommerce/docs/study/liability/finland_12nov2007_en.pdf.

b) *Interim measures and actions for injunctions under the Copyright Act*

In addition to the general rules on liability under Act 458/2002, in the specific case of civil actions for injunction and interim measures against ISPs, the provisions applicable are those of the Copyright Act (Act 404/1961),[88] which was amended by Act 679/2005 of 14 October 2005 to include a series of provisions (Articles 60a to 60d) designed to prevent access to copyright-infringing material.

Specifically, Article 60 a) envisages that, at the instance of the rightholders, the access or hosting provider must supply the court with information or contact data in any case where the subscribers to its services communicate files to the public which contain copyright-protected literary or artistic works. The applicant must show that a substantial amount of illegal material is being supplied from a specific customer's terminal (Article 60a.1), and must defray the costs incurred by the access provider (Article 60a.3)

The owners may subsequently -Article 60 b)- bring an action directly against the infringing end-user, using the data obtained following the latter's identification under Article 60a. In such a case, the court can order a halt to the infringing conduct and impose a conditional fine to reinforce compliance with the injunction.

Article 60c (1) also envisages an injunction that is directly filed against the intermediary, who must temporarily interrupt the end-user's access following the issue of the pertinent court order on pain of a fine.[89]

The plea to interrupt access can also be lodged as an interim measure in an action against the end-user, in any case where it is obvious that the owners' copyright would be in danger if the intermediary were not to interrupt access (Article 60c (2) of the Act). Although the measure will generally be taken after the court has heard both the party who made the notification and the owner of the content affected thereby, in cases of urgency it may even be adopted *inaudita parte* (Article 60c (3). At all events, the interim injunction lapses if a final injunction has not been sought against the infringing end-user within the space of one month -Article 60c (4)- and even where it is adopted by the court, the end-user cannot be barred from sending and receiving messages (e.g., by e-mail), a provision that is coherent with the fact that having access to a broadband Internet connection with a minimum of 1 MB per second has been deemed a fundamental right in Finland since 1 July 2010.

Apart from the ISPs' role in the case of actions and interim measures in the civil courts, copyright holders can also take action to instigate a criminal investigation of possible unlawful online posting of content pursuant to Act 493/1995,[90] a case in which the police (even without judicial support) can order the access provider to identify the alleged infringer.

[88] An English translation of the Act, updated to the reform of Act 307/2010, is available at website address <http://www.wipo.int/wipolex/es/text.jsp?file_id=208099>.

[89] The doctrine also states that, in Finnish copyright, an intermediary who collaborates in copyright infringement may be declared civilly liable for said infringement, in line with the general theory of non-contractual civil liability, though this would normally require strong causal implication in the damage. See OESCH, R., "Copyright Liability in the Internet from the Finnish Law Point of view", *Scandinavian Studies in Law*, 2002, vol. 42, p. 115.

[90] An English version of the Act, updated to Act 560/2007, can be found at website address <http://www.finlex.fi/fi/laki/kaannokset/1995/en19950493.pdf>.

2. Case-law

In Finnish case-law, pre-eminence must be given to the Finnish Supreme Court's decision in the *Finreactor I* case (decision of 30.6.2010)[91]. This held that seven administrators of the *Finreactor Bittorrent* portal which supplied hyperlinks for P2P applications were criminally liable. In its decision, the Court held that, despite the fact that the files were exchanged by the users themselves, and that such files were therefore neither stored nor reproduced by the Defendants, this in no way mitigated their criminal liability as accomplices or aiders and abettors, since the protection afforded by the Copyright Act does not depend on the way in which the unlawful exchange is technically executed.

The Supreme Court deemed that the corporate activity undertaken by the owners of the website was necessary for the end-users to be able to make the unlawful exchanges, and went on to state that the safe harbour for hosting service providers under Article 15 of the Act 458/2002 was not applicable because the Defendants participated directly in the infringing activity, and had actual knowledge of the fact that the creation and maintenance of the website served to enable the exchange of the protected files. Accordingly, the guilty parties were sentenced to pay a fine of 680,000 euros.

In a second decision handed down on the same day (*Finreactor II* Case),[92] the Finnish Supreme Court likewise found two individual end-users criminally liable for supplying large amounts of hyperlinks via the portal and thereby permitting other end-users to download copies of different files that contained computer games. The Court deemed that such conduct also rendered the unlawful files accessible to third parties, thus infringing the copyright of the holders pursuant to §2 and 56*bis* of the Intellectual Property Act.

In the sphere of the lower courts, the access provider *Elisa* has been forced to block customer access to *The Pirate Bay* website since January 2012, by virtue of Helsinki District Court Order of 26.11.2011.[93]

VII. FRANCE

1. Legislation

a) The Confidence in the Digital Economy Act

The Confidence in the Digital Economy Act of 21 June, 2004 (hereinafter referred to as the CDEA) (*Loi pour la Confiance dans l'Economie Numérique*)[94] transposed the DEC into French law,[95] governing exemption from liability for intermediaries.[96]

---

[91] (KKO: 2010:47), the decision is available at <http://www.finlex.fi/fi/oikeus/kko>.
[92] (KKO: 2010:47), the decision is available at website address <http://www.finlex.fi/fi/oikeus/kko/kko/2010/20100048>.
[93] See the press summary of the case at <http://www.edri.org/edrigram/number9.21/finnish-isp-block-piratebay>.
[94] The Act is available at website address <http://www.legifrance.gouv.fr/>.
[95] At a bill level, there is a report drawn up by Senators Béteille and Yung with respect to the application of the Anti-piracy Act (Act 2007-1544 of 29 October), which contains a recommendation (number 12) to amend the Directive on Electronic Commerce by introducing the category of "service editor" applicable to Web 2.0. intermediaries. The report proposes that the liability regime of such intermediaries ought to be something midway between that which corresponds to one who edits or publishes online content (subject to the rules of the *jus commune*) and that which corresponds to a "pure" hosting provider under Article 14 of the DEC. According to the report, these intermediaries should have an obligation to identify persons who, thanks to their services, post online content, an obligation in terms of

With respect to access providers and those who undertake mere data-transmission activities, Article 9.1 of the CDEA adds Article L-32-3-3 to the Postal and Electronic Communications Code (PECC) for the purpose of classifying these ISPs as "electronic communications services" and establishing a general rule of exemption from civil or criminal liability for any illegal content circulating in their networks, on the condition that such ISPs maintain a neutral attitude towards such content. To this end, the ISP must in no case initiate the transmission, select the receiver thereof, or select or modify the information transmitted.[97]

As regards *caching*, the CDEA also adds a new Article L-32-3-4 to the PECC, in order to exempt ISPs from civil and criminal liability in these cases, provided that they fulfil the conditions stipulated in the provision (i.e., not to modify the information, to comply with conditions on access to the website originally established by its operator, and not to hinder the data-collection technologies used by the website operator). ISPs may also exempt themselves from liability, if they act promptly to block or disable access to the information upon obtaining actual knowledge of the fact that the original files (i.e., those which were the subject of *caching*) have been removed from the network, or access to them has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Article 6.I.2 of the CDEA contains the exemption from civil liability for hosting service providers. This exemption extends to those who provide storage services free of charge or in consideration of a price, provided that they store the data at the request of the recipient of the service and do not have actual knowledge or awareness that the information is illegal or are not aware of facts or circumstances from which the illegal activity or information is apparent. They will similarly be exempt from liability if, upon obtaining such knowledge or awareness, they then act expeditiously to remove or disable access to the information.[98]

For civil liability purposes, Article 6.I.5 creates a presumption of bad faith for the hosting service provider in any case where it is notified in the manner envisaged under said Article of the illegal nature of the information. This notification must contain all the elements relevant to the case (date, full identity of the party that serves notice and of the recipient thereof, precise location of the disputed content, legal grounds which, according to the person serving notice, underpin said illegality, etc.).[99]

Nevertheless, Article 6.I.3 sets a stricter standard for criminal liability, since in this case the limitation of liability is only lost where there is actual knowledge of the unlawful nature of the material. Naturally, liability is likewise avoided by the hosting service provider who removes or disables access to the information as soon as it acquires such actual knowledge, pursuant to the provisions of Article 14 of the DEC.

---

means (not results) to monitor that the information stored is not illegal, to investigate any facts or circumstances that reveal said illegality, in line with existing technical means, and to make a reasonable effort to this end. It is likewise proposed that the operators of these platforms should be held liable (civilly or criminally) in any case where they have effective knowledge of manifestly illegal activities or content and fail to act promptly to remove or disable access to same. The report is available at <http://www.senat.fr/rap/r10-296/r10-2961.pdf>.

[96] In the wording in force following approval of Act No. 2011-267 of 14 March.

[97] Article 6.I.1 of the CDEA additionally requires access providers to inform their users that there are technical facilities which enable access to certain services to be restricted, and that there are means at the user's disposal to prevent the breach of the obligation established by Article 336-3 of the Intellectual Property Code (hereinafter referred to as the IPC).

[98] As envisaged under the Directive, the exemption from liability will not be applied in any case where the recipient of the service acts under the control or authority of the ISP.

[99] Article 6.I.4 of the CDEA provides for a prison sentence of up to one year and a fine of 15,000 euros in the case of any person who notifies an ISP of the existence of illegal content, knowing said notification to be false.

In addition, Article 6.I.7 (1) of the CDEA establishes the absence of a general obligation to monitor content or a duty to investigate facts or circumstances that might reveal the illegality of the information, something that is equally stated of access providers under Article 6.I.1 and hosting service providers under Article 6.I.2.

The LCNE, however, permits the courts to impose an *ad hoc* duty of monitoring or supervision on hosting service providers to prevent future infringements, in the case of material which is already effectively known to be infringing . At all events, such supervision may only be ordered by the court provided that it is temporary and for a specific case (Article 6 I-7 (2) of the LCNE).[100]

Lastly, Article 6.I.8 of the LCNE regulates interim injunction actions and measures, establishing their applicability to hosting service providers under Article 6.I.2 for the purpose of preventing or halting damage. Alternatively, these measures may also be targeted at access providers under Article 6.I.1.[101]

b) Other relevant enactments: HADOPI Acts and Intellectual Property Code.

The legal status of P2P software operators was extensively discussed during the parliamentary stage of what was to become the Information Society Copyright Act No. 2006-961 of 1 August 2006 (*Loi relative au droit d'auteur dans la société de l'information*),[102] which incorporated the provisions of the Directive 2001/29/CE into French law. During this stage, consideration was given to the possibility of "legalising" the conduct of these P2P network operators through the introduction of a compulsory licensing system, accompanied by a right of remuneration.

During its passage through the Legislative Assembly, however, the proposal was rejected, giving way to a new regulation in which the conduct of persons who make the means to exchange files over the Internet available to others was envisaged as a criminal offence under Article 335-2-2 of the *Intellectual Property Code* (IPC) (*Code de la Proprieté Intellectuelle*). The conduct of persons who design a programme *manifestly aimed at enabling the exchange of protected works and making it available to the public for this purpose*[103] is defined by this enactment as a criminal offence. The penalty provided for this offence is the same as that which corresponds to infringement of copyright and related rights.[104]

In the field of actions against direct infringers, while the statute known as the "HADOPI Act 1" (Act 2009-669 of 2 June 2009[105] to favour the dissemination and protection of

---

[100] In addition, Article 6.I.7 (3) contains special obligations imposed on ISPs with respect to a series of offences (crimes against humanity, incitation to racial hatred and violence, child pornography, etc).

[101] Article 6.II moreover requires ISPs to retain and preserve data that enable the persons who have created and transmitted the content (their customers) to be identified.

[102] J.O. 178 of 3 August 2006.

[103] LUCAS-SCHLOETTER, A., "*La Loi Française relative au droit d'auteur dans la société de l'information*", *Pe.i (revista de propiedad intelectual),* No. 25, 2007, p. 43.

[104] Sirinelli states that the law is aimed at holding those computer-programme publishers liable whose business model is clearly based on inducing the infringement of intellectual property rights. In this regard see SIRINELLI, P., "The Graduated Response and the Role of Intermediaries: Avoiding the Apocalypse or a Return to the Sources?", *Global Copyright*, Alai, 2010, p. 483.

[105] The Act (published in the *Journal Officiel* of 13 June 2009) originally contained a system that enabled an administrative board to receive the complaints of the owners and forward these to the access providers, who then had to send warning notices to their customers. If, after two such warnings, a user continued to exchange files, the Act empowered the Board to disconnect that user from the network for a maximum of one year. This system was declared unconstitutional by Constitutional Council Decision No. 2009-550 of 10 June 2009, published in the *Journal Officiel* on 13 June, on the grounds that disconnecting a user from the Internet required the intervention of a court, which led, in turn, to the drafting of the current Article 335-7 of the IPC.

creation on the Internet) introduced the "graduated response"[106] or "three-strikes"[107] system in France, it also added a new Article 336-2 to the IPC, which permits the court, at the instance of rightholders, to order service providers to take all the necessary measures to put a halt to an infringement or prevent it from happening.[108]

The injunction contained in this statutory provision may be directed against any person likely to be able to contribute to remedying the situation, which includes network access providers in those cases where this entails disabling access to P2P-hyperlink or video streaming sites.[109] The sole condition required by the French Constitutional Council for declaring the law in accordance with the French constitution is that the measures be adopted in the framework of an adversarial procedure and that they be proportionate.

For its part the HADOPI Act 2 of 28.10.2009 provided that, in the case of an offence against intellectual property committed over the Internet, a supplementary penalty would be applicable, consisting of suspension of the Internet connection for a maximum of one year, a ban on entering into another Internet access contract with the same or any other operator, and payment of the cost of the suspended service.

2. Case-law

The French courts have handed down decisions on the question of ISP liability, which could generally be described as varied and, at times, contradictory. Given the large numbers involved, judicial rulings (orders or decisions) of the Courts of First Instance will be omitted and only those of special relevance issued by the Court of Cassation (*Cour de cassation*) or Appeal Courts will be highlighted.

a) *ISP liability*

With reference to the liability of hosting service providers, special mention should be made -in view of it being the first to address the matter -[110] of the decision of the Court of Cassation (Civil Chamber 1) of 14.1.2010[111] (*Tiscali* case). The case arose from the action brought in 2002 by two publishing houses against *Tiscali Media* (currently

[106] In reality, the Act starts from the basis of attributing liability to the user, by establishing that criminal negligence exists (be it only *in vigilando*) if, despite the warnings, exchanges of illegal material continue to be made from his/her connection. Specifically, Article L 336-3 paragraph one of the IPC provides that the owner of the connection has a monitoring duty to ensure that it is not used to violate copyright.

[107] The currently prevailing system consists of giving an administrative authority the task of requesting the courts to order the halting of the Internet connection service in respect of users who have repeatedly been warned that the exchange of files constitutes infringing conduct. For the purpose, the *HADOPI* is required to contact 9 courts distributed throughout France to furnish the information available, with the court in question then being tasked with imposing the penalty, after fast-track proceedings without oral submissions and *inaudita parte*. The administrative body is also responsible for enforcing the penalty on the subscriber, who, despite not having a network connection, will nevertheless retain television and telephony services in the case of packages sold in unit form.

[108] The Act also adds a new modality of copyright infringement by users, on Article 335-7-1 of the IPC introducing a infringement due to gross negligence in the case of users who have failed to implement the necessary measures to prevent violation of rights from their Internet connection, in any case where they have been duly notified that said connection is being used for infringing purposes.

[109] LUCAS-SCHLOETTER, A., "Google face à la justice française et belge", *Journal of Intellectual Property, Information Technology and E-Commerce Law*, vol. 2, 2011, p. 148.

[110] In reality, the provision applied by the Court of Cassation in this case was that in force before the CDEA, i.e., Article 48-3 of Act No. 86-1067 of 30 September 1986, in the wording conferred by Act 2000-719 of 1 August. However, the similarities between the previous regime and that now in force render the doctrine of the judgement valid because, already at that time, the Act departed from the premise that there was an exemption from liability for hosting service providers who had no control over the housed content, an exemption which was lost if the provider was not diligent in removing or disabling access to such content.

[111] Case 09-18855. The decision is available at website address <http://www.legifrance.gouv.fr/> and in *Revue Internationale du Droit d'Auteur (RIDA),* No. 223, 2010, pp. 456-466.

Telecom Italia) because a comic had been illegally reproduced and communicated on one of the websites hosted by this ISP.[112]

In the case, the question arose as to whether *Tiscali* had been in breach of its obligation to identify those responsible for the infringement (the information furnished by the end-user to the provider was obviously false)[113] and whether it had relinquished its passive role by virtue of supplying a service whereby end-users could design their own web pages (in the case in point, the infringer had used this service) and then insert advertising into such pages with which a financial reward was obtained. The Court of Cassation held that the gain obtained and web page-design service went beyond mere technical intervention, which meant that in this specific case the provider was not entitled to enjoy the exemption from liability and was thus liable for the Claimants' copyright infringement.

b) Web 2.0 intermediation activities

With respect to the question of liability of Web 2.0 electronic platform operators, attention should be drawn to the Court of Cassation decision of 17.2.2011[114] in the *Dailymotion* case (a service similar to *YouTube*, targeted at the French market).

The Court of Cassation stated that the service provided by *Dailymotion* was essentially passive, since it took no part in the activity of uploading and downloading audiovisual material in which end-users engaged on its electronic platform. The fact that *Dailymotion* obtained a financial reward from the commercial exploitation of advertising did not detract from this in any way (an issue on which the CJEU doctrine in the *Google France* case -to which reference will be made below- made its influence felt).

Accordingly, the Court of Cassation held that the intermediary could benefit from the exemption from liability envisaged under Article 6.I.2 of the CDEA for hosting service providers, an exemption that remained valid due the fact that the rightholders had failed to give adequate notification of the precise location of the infringing videos. In the face of said lack of notification, the platform operator had not had the opportunity to comply with its obligation to act diligently by removing the infringing content or blocking access to same.

Similarly noteworthy were the four decisions handed down by the Paris Court of Appeal on 19.01.2011 concerning the *Google Videos* service.[115] In all cases, the rightholders detected that various audiovisual recordings containing motion pictures were available to the remaining users, both through the provision of hyperlinks and by means of being stored on *Google Videos*' servers.[116]

In this case, the Claimants, rather than directly seeking to make the Web 2.0 platform operator liable by challenging the application of the safe harbour afforded to *hosting* under the CDEA, opted instead to use the procedure introduced by the "HADOPI Act" in the IPC, by informing the intermediary of the existence of the videos, which were immediately removed. Subsequently, however, the owners discovered that there were

[112] See the commentary in SIRINELLI, P., *Revue Internationale du Droit d'Auteur (RIDA)*, No. 223, 2010, pp. 417 ff. and in MATULIOYITÉ R., and NÉRISSION, S., "The French Route to an ISP Safe Harbour, Compared to German and US. Ways", *IIC,* No. 42, vol. 1, pp. 55 ff.

[113] Tiscali supplies information in which "comic" appears as the name of the owner of the web page, and "comic street" as the address.

[114] *Societé Nord-Ouest & UGC Images. v. Dailymotion*, decision of 1 Civil Court, case number 09-67.896, available at website address <http://www.juriscom.net/jpt/visu.php?ID=1291>.

[115] The decisions (relating to the documentaries "l'affair Clearstream", "Le génocide arménien", "Les dissimulateurs" and "Mondovino") are available at website address <www.legalis.net>.

[116] In 2011 Google announced that it was eliminating the possibility of "downloading" videos stored from that date onwards but at the time when the events occurred such downloading was possible.

still hyperlinks to the infringing material, and that (in at least two of the cases) the videos had been replaced by other end-users, which led to the action for copyright infringement being brought against the US parent company and the French subsidiary.

The Paris Court of Appeal recognised the close connection between the service of providing hyperlinks to videos and that of storing the latter on a server, analysing whether the two, taken together, came within the description of "provision of hosting" contained in Article 6.I.2 of the CDEA. The Court concluded that it did, holding that this amounted to a process automated by end-users, over which the intermediary had no control, and that this, in turn, accorded with the requirement of neutrality under Article 14 of the Directive.

Nonetheless, it also stated that the search-engine operator was, not only required to act promptly and diligently to remove the videos in question, but also had an *a priori* duty to act, by using all the technical means at its disposal to prevent any possibility of said videos (the infringers) being re-uploaded to the service (*notice and stay down* process).[117] Accordingly, since in this specific case copies of the unlawful videos had not been prevented from being re-housed on its servers, the intermediary could not avail itself of the Article 6.I.2 exemption from liability, with the result that the *jus commune*, and specifically the rules of attribution of civil liability enshrined in Articles L-335-3 and L-335-4 of the IPC, were applicable.[118]

There have been a number of decisions by the Paris Court of Appeal in another series of cases relating to Web 2.0 platform activity (three decisions of 3.9.2010[119] and another of 23.1.2012),[120] which held the company *Ebay International* (operator of the French *Ebay* site) liable for the exchange between private individuals of clothing and other articles which infringed the Respondents' trade mark rights. The Court deemed that the online marketplace operator had engaged in conduct of an active nature and that it had obtained a financial gain, not only from the data stored, but also from the pirated merchandise auctioned, which barred it from benefiting from the exclusion of liability envisaged under Article 14 of the DEC.

This doctrine has also been recently adopted by the French Court of Cassation, which in three decisions of 3.5.2012[121] (upholding those of the Paris Court of Appeal of 3.9.2010 outlined above) held that, far from engaging in a simple hosting activity which was totally independent of the activity of the vendors of counterfeit products, the operator of the online auction site instead played an active role which gave it sufficient knowledge or control of the information that it hosted, and so deprived it of exoneration from liability under Article 6.I.2 of the Act of 21 June 2004 and Article 14.1 of the DEC.

---

[117] See LUCAS-SCHLOETTER, A., "*Google face à la justice française et belge*", cit., pp. 145-147.

[118] The doctrine has indicated that, in accordance with the traditional rules of the *jus commune*, intermediaries may be deemed infringers of copyright in any case where they have a sufficient degree of collaboration in the criminal act. See GINSBURG, J.,/GAUBIAC, Y., "Contrefaçon, fourniture de moyens et faute: perspectives dans les systèmes de *Common Law* et civilistes à la suite des arrêts *Grokster* et *Kazaa*", RIDA, 2006, No. 207, p. 47.

[119] *Ebay Inc, Ebay International v. Christian Dior Couture,* available at website address <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2970>, *eBay v. Parfums Christian Dior, Kenzo Parfums, Parfums Givenchy, Guerlain,* available at <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2972> and *Ebay Inc, eBay International v. Louis Vuitton Malletier AG,* available at <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2973>.

[120] In *eBay International v. Burberry Ltd and others*, available at <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3346>.

[121] Available at website address <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3398> (*Ebay Inc, eBay International v. LVHM and others*), <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3401> (*Ebay Inc, eBay International v. Louis Vuitton Malletier AG)* and <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3400> (*Ebay Inc, Ebay International v. Christian Dior Couture).*

c) *Internet search engines*

The decision in the *Tiscali* case caused a great stir in the press in France but its doctrine (at least as far as liability for copyright infringement is concerned)[122] has nevertheless been counteracted to a certain degree by the decision of the Court of Justice of the European Union of 23.3.2010 (*Google France* case).[123]

In this decision, the CJEU, in response to a question referred for a preliminary ruling by the French Court of Cassation in a case of trademark right protection, held that the provision of advertising services for profit by an Internet search-engine operator (in this case the hyperlink service sponsored by *Google*) in no way barred said search-engine operator from benefiting from the exception of liability envisaged under Article 14 of the DEC for hosting service providers.

The Claimants in the case, the rightholders of a trademark for fashion goods and accessories in France, pleaded that when their trademarks were entered into the search engine, along with the results naturally yielded by the search engine there appeared sponsored hyperlinks (paid for by the owner of the linked web page) which directed browsers to the web pages of competitors.

With respect to the exemption from liability, the CJEU stated that Article 14 of the DEC (via Article 6.I.2 of the CDEA) also protects Internet search engine operators (providers of online reference services) in any case where they do not play an active role that can give them knowledge or control of the information stored.[124] In the absence of such an active role, the search-engine operator cannot be deemed liable for the advertisements inserted into the web page by its customers, unless, after becoming aware of the illegality thereof, it should then fail to act expeditiously to remove such content or disable access to same.[125]

In essence, this decision means that the advertising service operated by an Internet search-engine operator *can benefit from the* exemption from liability envisaged under Article 14 of the DEC, where the operator of the service continues to have a passive (technical or neutral) role,[126] something that must ultimately be determined by the domestic court. The CJEU's final solution is thus open-ended, with intermediary's neutral or non-neutral status for the purpose of being eligible to benefit from the exemption from liability under Article 14 of the DEC depending, according to the Court, on very specific factual aspects that have to be ascertained by the domestic courts.

---

[122] Not, however, as regards the obligation to identify the infringing user, in respect of which the doctrine handed down by the Court of Cassation in *Tiscali* remains in force.

[123] *Google France, Google Inc, v. Louis Vuitton, Viaticum et al.* Cases C-236/08, C-237/08, C-238/08, available at website address <http://curia.europa.eu/>.

[124] The CJEU's decision also directly affects the doctrine established by the Court of Cassation in the *Tiscali* case, where the denial of the *hosting* safe harbour took into account, as a fundamental element, not only the technical intervention entailed in developing a system whereby users could create their own web pages, but also the fact that the advertising inserted implied a business model that was incompatible with the activity assigned to a "traditional" hosting provider. Now, however, the CJEU in the *Google France* case has allowed that services which include advertising may still benefit from the safe harbour for hosting, provided that they maintain a neutral position with regard to the content, something that can only be analysed on a case-by-case basis, and not *a priori*.

[125] The Court of Justice also held that the fact that the order in which the advertisements appeared on the screen was controlled by the search engine operator (depending on the amount paid) in no way implied the existence of an active role or control. Similarly, the fact that the service was remunerated and that the search engine operator set the manner of remuneration was likewise not indicative of such control.

[126] Surprisingly, in its reasoning the CJEU cited Preamble 42 to the Directive on Electronic Commerce 2000/31, which is nevertheless applicable solely to activities of mere conduit (data-transmission and access) and not to those of hosting.

Applying this doctrine, on 13.07.10 the Commercial Chamber of the French Court of Cassation handed down four decisions[127] in cases very similar to that decided by the CJEU (owners of national or community trademarks who claimed that, by way of results, the online trademark search yielded advertisements that directed users to the web pages of their competitors). In all four cases, the appeal decisions held that *Google* was not entitled to benefit from the exemption from liability under Article 14 of the DEC (Article 6.I.2 of the LECN), in view of the fact that its function as an advertising service differed from its function as a mere search engine, exceeding a merely neutral role.

The Court of Cassation did not, however, resolve the issue. It simply held that the Appeal Courts had not taken the CJEU doctrine in the *Google France* case into account, so that they had to decide anew in order to ascertain whether in each of the cases the search-engine operator had a passive (technical or neutral) role that would enable the application of the safe harbour pursuant to Article 14 of the DEC.[128]

In this regard, it should be borne in mind that the Paris Court of Appeal itself, in a separate "*Google France* case" unconnected with these four (decision of 19.11.2010),[129] had already indicated that the fact that the information stored was not for commercial purposes was no bar to the search-engine operator benefiting from the exception under Article 14 of the DEC, and that in this specific case, *Google* had no knowledge of the illegal nature of the information furnished by the advertiser, thus passing the requisite test of neutrality for being eligible to seek haven in the *hosting* "safe harbour".

In addition, there have been at least three other subsequent decisions concerning the activity of search-engine operators under French law, in which the influence of the CJEU's decision in the *Google France* case has been felt.

The first two involved decisions of the Paris Court of Appeal of 26.01.2011[130] (*Saif v. Google*) and 04.02.2011[131] (*Google v. Aufemenin.com*), in which the question was raised of the lawfulness of the *Google Images* service, where, in response to certain key words being entered, the search engine displayed small-scale images (thumbnails) which, according to the Respondents, infringed the copyright of those who had taken the original photographs and posted them on their respective web pages.[132]

In the *SAIF* case, the Court of Appeal rejected the existence of the search-engine operator's liability for the *Google Images* service. The Court held that the copies stored on the search engine's servers[133] were reproductions of works that were then

---

[127] Cases 05-14331, 08-13944, 06-20232 and 06-15136. The decisions are available at website address <http://www.legifrance.gouv.fr/>.

[128] See a complete judicial history of the case in BEDNARZ, T., "Keyword Advertising Before the French Supreme Court and Beyond", *IIC*, 2011, pp. 652-653.

[129] *SARL Google France v. Syndicat français de la literie*, *IIC*, 2011, p. 742.

[130] Case RG No. 08/13423, available at website address <http://www.juriscom.net/documents/caparis20110126.pdf>.

[131] Case RG No.09/21941, Google France v. Aufemenin.com and others, available at <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3119>.

[132] In both decisions, the conclusion was reached that the law applicable to the case was French law, rejecting the position adopted by the lower court in one of the cases to the effect that the law to be applied was US law, which, according to the court, would permit *Google* to undertake this type of reproduction under the fair use doctrine.

[133] In reality, it is debatable to maintain that the images shown on the *Google Images* service are reproduced on the search engine operator's server. Normally, search engines store copies of the HTML code of the web pages, i.e., text, on their servers, displaying the images by means of inline links without actually reproducing them on their own servers. Hence, despite the fact that the end-user has the impression that the images shown "are" on the search-engine servers, this is not so from a technological point of view: it is a mere visual impression (each image continues to be stored on its "original" server).

communicated to the public and accessible from France. It nevertheless found that the search-engine operator was not liable for such acts of unauthorised exploitation, though to arrive at this conclusion it did not apply the safe harbour under Article 14 of the DEC (as it would subsequently do, however, in the *Aufemenin* case), but instead pragmatically resorted to the idea that the reproductions of the images were transient and provisional, using -though without applying it directly or expressly- the terminology of the exception cited in Article 5.1 of Directive 2001/29/CE.

In the *Aufemenin.com* case, the selfsame Paris Court of Appeal (albeit sitting in a chamber different to the one that rendered judgement in the *SAIF* case) began by dismissing the search-engine operator's contention that authors who placed images on the Internet were tacitly or implicitly giving their consent to the small-scale reproductions produced by search engines. The Paris Court of Appeal nonetheless stated that the search-engine operator could indeed benefit from the exemption from liability established for hosting service providers under Article 14 of the DEC, in view of the fact that the search for and display of images is a totally automated process over which the intermediary has no degree of control whatsoever.

Even so, search-engine operators are also under an obligation, not only to remove any content that infringes Claimants' copyright at said Claimant's request, but also to conduct active monitoring of the network to prevent content that has been withdrawn from again being posted online (*notice and stay down* process).[134] Hence, in this case, the Court found that there had been an infringement of reproduction rights and the right of communication to the public (in the form of "making available") in respect of such material as had been removed and re-uploaded, which generated the corresponding liability.

Lastly, with respect to pure (word-based) search activity, mention should be made of the Paris Court of Appeal's decision of 3.5.2011.[135] This stated that, when a user started writing a word, the fact that the search engine might, by way of search terms, suggest the names of hyperlink pages or electronic platforms targeted at exchanging files between end-users implied no liability whatsoever on its part,[136] since said system was based on an automatic algorithm which imbued the search-engine operator with a clearly passive role.[137]

VIII. GERMANY

1. Legislation

The provisions of the Directive on Electronic Commerce governing limitations of liability for ISPs in respect of infringements of various legally protected rights, including intellectual property rights, were implemented in German law by Articles 7 to 10 of the German Telemedia Act of 26 February 2007[138] (TMA) (*Telemediengesetz*, reformed by Act of 31 May 2010).

---

[134] See LUCAS-SCHLOETTER, A., "*Google face à la justice française et belge*", *Journal of Intellectual Property, Information Technology and E-Commerce Law,* vol. 2, 2011, pp. 145-147.

[135] *Snep. v. Google,* RG No. 10/19845, available at website address <http://www.pcinpact.com/media/Google%20SNEP%20arret%20CA%20Paris%203%20mai%202011.PDF>.

[136] Furthermore, this same decision held that Article 336-2 of the Intellectual Property Code may only be used against a person to the extent to which he/she might be eligible to contribute to remedying the infringement, something that did not occur in this case (given that, even though the search engine operator made no search suggestion, the browser could equally arrive at the websites and download the illegal content from them).

[137] The avenue used in the case was an action for injunction under Article 336-2 of the Intellectual Property Code, as worded by the " HADOPI Act " of 12 June 2009.

[138] Official Gazette I, p. 179.

The TMA is predicated on the general principle of liability for any party directly supplying online content -§7 (1)- and goes on to implement Article 15 of the DEC at §7 (2) 1, which stipulates that there is no obligation to monitor content transmitted or stored or to investigate circumstances that might indicate illegal activity. In addition, the Act states that the rules of liability are established without prejudice to any possible action for injunction, which remains untouched pursuant to §7 (2) 2.

§8 of the TMA contains the exemption from liability for activities of provision of access and mere transmission of information (mere conduit),[139] requiring ISPs to abide by the conditions laid down in Article 12 of the DEC, namely, in no case to initiate the transmission, to select the receiver thereof, or to select or modify the information transmitted. Under the terms of the Directive, the exemption from liability will not be applied in any case where the recipient of the service acts under the control of or jointly with the ISP.[140]

§9 of the TMA establishes an exemption from liability for system or proxy caching activities (caching to accelerate transmission, in the words of the clause heading), if a series of conditions that reproduce the provisions of Article 13 of the DEC are fulfilled (no modification of the information, compliance with conditions on access to the information established by the owner of the cached page, compliance with rules regarding the updating of the information, etc.). This includes the obligation flowing from Article 13 e) of the DEC to remove or disable access to the information stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered the removal or disablement of such cached information.[141]

Lastly, Article 10 of the TMA establishes the safe harbour for hosting service providers, requiring that, in order to gain exemption from criminal liability, service providers have no actual knowledge that the activity is unlawful or (with respect to compensation for damages) know of no relevant facts or circumstances that render the unlawful nature of the wrongful act obvious.[142] Recourse may also be had to this exception by hosting service providers who, upon somehow learning of the illegal nature of the activity, swiftly proceed to disable access or remove the data. Pursuant to the Directive, the exemption will not be applicable in any case where the recipient of the service acts under the control of or jointly with the hosting service provider (§10 (2) TMA).

With reference to specific legislation governing intellectual property, according to German legal doctrine, §97 of the Copyright Act (CA, or *UrhG* in its German

---

[139] It must additionally be borne in mind that Article 5 of the TMA excludes ISP liability for Internet traffic management activities via routers or gateways, taking it as read that, as stated by Preamble 43 to the DEC, the merely technical handling of data that such activities require (e.g., their being split into packages) implies no modification of the information in the sense of Article 12.1 of the DEC.

[140] Paragraph two of this paragraph 8, like Article 12.2 of the Directive, establishes an exemption from liability for providers who make transient copies of the information that they transmit.

[141] In its final subsection, 9 (1) states that the section which regulates the conditions for exemption from liability for access providers and network operators shall not be applied in any case where the service provider *deliberately* collaborates with one of the recipients of the service in order to carry out illegal activities.

[142] It has been said that in the criminal field there is no liability in cases of reckless disregard or merely negligent ignorance, in view of the difference between "knowledge" and "effective knowledge" being omitted from the TMA. In the field of civil actions for compensation, however, liability also arises in cases of criminal negligence. In this connection, see VV.AA. "Study of the Liability of Internet Intermediaries", p. 37, available at <http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf>.

abbreviation) includes cases of infringement through participation,[143] i.e., resulting from joint causation of damage,[144] leading to actions for compensation and to actions for injunctions that can extend to ISPs. Accordingly, this involves direct liability, which requires *mens rea* or gross negligence in cases where the infringement is so glaring that the ISP is unable to ignore it (e.g., because reiterated notifications have been received from the aggrieved rightholders). This includes attributing liability to any party that collaborates in bringing about the damage in a general capacity by, for instance, acting as an accomplice, aiding and abetting, or inducing or procuring the commission of an infringement.

2. Case-law

In Germany, a great number of decisions have addressed the question of the liability (civil and criminal) of Internet intermediaries. Consequently, this report will refer to the most important of these, corresponding to judgements handed down by the German Supreme Court (*Bundesgerichtshof*-BGH), though occasionally reference will also be made to especially relevant decisions issued by Regional Appeal Courts (*Oberlandgericthshof*-OLG).

German case-law contains some singularities in the case of ISP liability,[145] since there is a clear duality between actions seeking damages or criminal liability on the one hand[146] (in which the rules of the TMA are applicable), and interim measures and civil actions for injunction on the other, in which the rules applicable are those of the *jus commune* and of the *Störerhaftung* doctrine in particular[147] (translated into English as "disturber's liability"), which has been developed by the German Courts in different cases of infringement of immaterial rights or unfair trade practices, with the aim of widening the range of civilly liable persons in the face of the impossibility of determining direct infringement or infringement by participation in line with the rules of the CA and TMA. This doctrine fundamentally consists of applying certain duties of control over illegal content to ISPs (and hosting service providers in particular),[148] if a series of circumstances detailed in BGH case-law is present.

---

[143] It must further be borne in mind that in the *jus commune* §830 (1) of the German Civil Code provides that, in any case where two or more persons jointly cause damage, each of them will be liable for the damage, a rule that also applies where it is not possible to ascertain which of the various participants caused the damage. Additionally, §830 (2) clarifies the fact that any person who incites or acts as an accomplice will be deemed to be equivalent to a co-perpetrator of the damage. §840 (1) lays down that in such cases the obligation is joint and several.

[144] SPINDLER, G., and LEISTNER, M., "Secondary Copyright infringement: New perspectives in Germany and Europe", *IIC*, 2006, vol. 7, p. 796.

[145] These providers, moreover, have an obligation to inform the administrative or judicial authority of the identity of the users of their services in cases of serious offences (§100a (1) of the Criminal Procedure Code) and possibly also (though this is discussed in the doctrine) in the case of merely civil actions, dating from the amendment of §101 (2) of the Copyright Act, in accordance with the special process established at §101 (9). In this regard see CZYCHOWSKI, C., and NORDEMANN, J., "Use of Retained Data and Copyright Law in Germany", *European Intellectual Property Review*, 2010, p. 175.

[146] Basically for incitement to hatred (§130 of the Penal Code), dissemination of violent images (§131 of the Penal Code), distribution of pornography (§184 of the Penal Code) and abuse (§185 of the Penal Code). See HOEREN, T., "German Law on Internet Liability and Intermediaries", *LIDC Congress 2011*, available at <http://www.wettbewerbszentrale.de/media/getlivedoc.aspx?id=31684>.

[147] The generous use of this doctrine in German law is in part explained by the fact that the statute implementing Directive 2001/29/CE in Germany does not establish in the country's national law the possibility of filing for interim measures and bringing actions for injunction against ISPs for copyright infringement.

[148] In general, German case-law lays down that there is no obligation on access providers to block content or implement any filtering thereof, since there is no causal connection with the copyright infringement committed by users and this would amount to intervening in constitutionally protected private communications. It is however possible for access providers to be requested for information about infringers, pursuant to §101 (2) of the Copyright Act. See HOEREN, T., "German Law on Internet Liability and Intermediaries", cit., pp. 6 and 14.

These circumstances are, in essence, that the indirect infringer (*Störer*) has wilfully contributed to the infringement with sufficient causal contribution,[149] that said party had the possibility of preventing the damage caused by the principal infringer by taking reasonable measures from a technical and financial standpoint;[150] and that there has been a breach of a duty of care or monitoring vis-à-vis content,[151] which implies having knowledge of the infringement committed (e.g., through notification from the aggrieved party) or that said infringement was clearly or evidently committed.[152]

a) *ISP liability*

i. Actions for injunctions and application of the *Störerhaftung* doctrine.

When the *Störerhaftung* doctrine is applied to the concrete case of ISPs, the German courts[153] have laid down that hosting service providers (including interactive Web 2.0 platform operators within this concept) are required to monitor content matter in any case where they have actual knowledge of its illegality through a judicial decision or certified notification from the aggrieved rightholder. From this juncture onwards, there is an active obligation to undertake monitoring, so as to ensure that end-users do not again upload clearly unlawful content matter to the web page or Web 2.0 platform for which they provide hosting or technical support, thereby preventing a repetition of the infringement.

Logically, this duty does not include any *a priori* general obligation to monitor all content matter, something that would be incompatible with Article 15 of the DEC. It solely requires the provider to remove the infringing material and take measures to prevent said material (i.e., files which contain *the same* protected literary and artistic works) from again being uploaded to the Internet.

Nevertheless, the specific scope of this monitoring obligation has still to be comprehensively defined by case-law. It is said to include all technically possible and economically reasonable measures to prevent future infringements, though these requirements have not been spelled out by the German legislature.

The three key decisions on this issue are drawn from the field of trademark rights. The first of these (the true leading case on the matter) was that handed down by the BGH on 11.3.2004 in the *Internet Auction I* case,[154] where the well-known watchmaker, *Rolex*, claimed that the online *Ricardo* auction site was liable for unauthorised trademark use as a result of the auctioning of counterfeits on an online marketplace.

Applying §10 of the TMA (Article 14 of the DEC), the BGH rejected the existence of civil or criminal liability insofar as the intermediary was concerned. It nevertheless made it clear that said exemption from liability did not affect the injunction and, specifically, the duty resting on the ISP not only to remove infringing content from the system, but also to prevent future infringements.

---

[149] See the BGH's decision of 17.8.2011 in the *Stitparfüm* case, *GRUR 2011*, pp. 1038 ff., available on the BGH's own web page at <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=57743&pos=0&anz=1>.

[150] See HOEREN, T., "German Law on Internet Liability and Intermediaries", cit., p. 2.

[151] See NORDEMANN, J.B., "Liability for Copyright Infringements on the Internet", *JIPITIC*, No. 2, 2011, pp. 39-40.

[152] BGH's decision of 15.10.98, *GRUR* 1999, pp. 418 ff., in the *Möbelklassiker* case.

[153] This is an idea developed by BGH case-law since the 1960s in different cases relating to intellectual property and unfair trading. See SPINDLER, G., and LEISTNER, M., "Secondary Copyright infringement: New perspectives in Germany and Europe", *IIC*, 2006, vol. 7, p. 794.

[154] *Rolex v. Ricardo*, *JurPC Web-Dok*, 31, the text of the decision is to be found available at <http://www.jurpc.de/rechtspr/20040265.htm>.

An obligation thus arises whereby the auction website operator must both remove content which, according to duly certified notification, infringes trademark rights, and take measures to prevent similar infringements occurring in the future, provided that such measures are possible (realistic) and financially reasonable.[155] In the specific case of the wrist-watch trademark, this meant that the online auction site was required to monitor any future auction of articles carrying said trademark (e.g., by implementing a filtering system).

The essence of this doctrine was subsequently reiterated by the BGH's decision of 19.4.2007 (*Internet Auction II* case), in which the watchmaker's action was brought against the *Ebay* auction site. By way of a general rule, the BGH laid down that, while imposing a general monitoring obligation would make this type of company's business model impossible, it was not however incompatible with the establishment of specific obligations in response to notifications of infringements of third-party rights, which sufficed for the ISP to be deemed duly advised of the occurrence of the infringement. This, in turn, meant that the ISP would thenceforth be required to take all such measures as were reasonable from a technical point of view to prevent future infringements.

Lastly, in a third case of trademark right infringement (in this instance by the online auction of perfumes), the BGH's decision of 17.8.2011 in the *Stitparfüm* case[156] once again repeated the fact that ISPs had an obligation to take the necessary measures to prevent new infringements of third-party rights from occurring in the future, though this in no way implied a duty to subject all web-page traffic to prior monitoring.[157]

With respect to copyright infringements, the decision of the Hamburg OLG of 30.9.2009 (*Sharehoster* II case)[158] stated that, though hosting service providers were protected in actions for civil or criminal liability thanks to Article 10 of the TMA, under the *Störerhaftung* doctrine these ISPs had to carry out active searches, both manual and automatic, to check whether there were infringing materials that had previously been identified as such. Companies also had to check all content placed in the system by any user who had previously been detected as being an infringer (repeat offender).

In a subsequent decision of 14.3.2012 (*Rapidshare II* case),[159] the Hamburg OLG held that, with respect to a digital storage service in which end-users could house content matter for downloading by others, the owner of said storage facility had the obligation to carry out active monitoring of any content duly identified as unlawful by means of the appropriate notification, so as to prevent the possible reappearance of hyperlinks in the

---

[155] SPINDLER, G., and LEISTNER, M., "Secondary Copyright infringement: New perspectives in Germany and Europe", *IIC*, 2006, vol. 7, p. 794.

[156] *GRUR 2011*, pp. 1038 ff., available on the Internet at <http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=57743&pos=0&anz=1>.

[157] There is another BGH decision of 28.08.10 in the *Hartplatzheld* case, in which the Court held that there was no act of unfair trading where a website allowed users to upload and download videos of regional divisional football games, even though the broadcasting rights in these games did not belong to said website. The decision, with an introduction in English by D. JLUSSI, is available in 3, *JIPITEC (2011),* p. 150, at <http://www.jipitec.eu/issues/jipitec-2-3-2011/3179>.

[158] The decision is available in *Multimedia und Recht*, 2010, pp. 51 ff., and on the Internet at <http://dejure.org/dienste/vernetzung/rechtsprechung?Text=MMR%202010,%2051>.

[159] The decision jointly settles two actions brought by the rights management society, GEMA, and by two book publishers, and is available on the Internet at website address <http://www.telemedicus.info/urteile/Internetrecht/Haftung-von-Webhostern/1356-OLG-Hamburg-Az-5-U-8709-Rapidshare-II.html>. The lower court decision (*LG Hamburg* 2.7.2008) is available in *Multimedia und Recht*, 2008, pp. 823 ff.

system which would target these infringing files.[160] The Court also ordered the website operator to conduct selective active searches for the purpose of detecting further possible infringing content.

Nonetheless, the Düsseldorf OLG's decision of 27.4.2010[161] (*Rapidshare I* case), where the facts of the case were very similar to those adjudged by the Hamburg OLG, deemed the preventive measures adopted by the Defendant to be reasonable and adequate for preventing the infringement,[162] thus lending the ISP a neutral character. The Düsseldorf OLG stated in particular that hosting service providers had no obligation to act proactively to review material exchanged by end-users and remove infringing material, or to implement key-word filtering to prevent the infringements committed by their users. Furthermore, the Zweibrüke OLG's decision of 14.5.2009[163] ruled that the operator of an Internet forum had no duty to control each and every entry made by end-users.

In a more recent decision, once again in relation to Web 2.0 intermediation activities, the decision of the Hamburg *Landgericht* (Court of First Instance) of 20.4.2012[164] (*GEMA v. YouTube*)[165] held that copyright infringement by a series of videos posted on the platform had been proved. This liability fundamentally flowed from the fact that *YouTube* only removed the videos seven months after the date of the initial notification from GEMA, a period of time that was not consistent with a diligent or swift reaction. The Court further held that, in conformity with the *Störerhaftung* doctrine, it was reasonable to require *YouTube* to undertake computerised filtering of videos that had already been identified as infringing, as well as key-word filtering to detect new copies of such infringing videos.

In the specific case of *Usenet* service providers, the Hamburg OLG's decision of 14.1.2009[166] held that, in this instance, the ISP carried out an activity similar to that of access providers, so that it had a duty of preventing infringement in accordance with the *Storërhaftung* doctrine only after having been informed of the copyright infringement by the rightholders. However, the Düsseldorf OLG's decision of 15.1.2008[167] held that, in this case, *Usenet*'s conduct was more akin to a type of activity such as the provision of *caching* services under §9 of the TMA

ii. Actions for compensation as direct infringers.

In addition to the imposition on ISPs of duties of monitoring and prevention of future infringements, the German courts have also held that ISPs were civilly liable in a

[160] The Court ascribed special value to the fact that, in the past, *Rapidshare* had a downloading incentive system consisting of offering a financial reward to users who had uploaded files that were downloaded a great number of times.
[161] The decision is available in *Multimedia und Recht*, 2010, pp. 483 ff. and at website address <http://www.jurpc.de/rechtspr/20100128.htm>.
[162] Specifically, this was a system for filtering files that were identical to those already deleted and an "Abuse service" which examined owners' complaints about material that they viewed as infringing their rights.
[163] The decision is available in *Multimedia und Recht*, 2009, pp. 541 ff. and at website address <http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1961>.
[164] Available at <http://openjur.de/u/311130.html>.
[165] In the case, the rights management society, GEMA, brought an action against the *YouTube* platform for 12 videos uploaded by users, in which the lyrics and music of different songs (including the well-known "By the Rivers of Babylon" by Boney M) were illegally reproduced.
[166] ZUM-RD, 2009, pp. 246-257, available at website address <http://www.telemedicus.info/urteile/Internetrecht/Filesharing/733-OLG-Hamburg-Az-5-U-11307-Haftung-des-Usenet-Providers-fuer-Urheberrechtsverletzungen.html>.
[167] Available at website address <http://www.elbracht.net/uploads/media/080129_OLG_Duesseldorf_I_20U95_07.pdf>.

number of cases in which the rules of the TMA were not applicable, due to the fact that they involved direct infringement by the intermediaries themselves.

This, for instance, was the case of the BGH's decision of 12.07.2007,[168] in which the German Supreme Court held that the liability attributable to an online auction platform for the sale of obscene content did not flow from the *Störerhaftung* doctrine of §1004 of the Civil Code, but rather from direct infringement of the provisions of the Unfair Trade Act (specifically, from the breach of due diligence in its professional work as an online intermediary).

In a subsequent decision of 12.11.2009 (the *Marions KochBuch* case)[169] relating to Web 2.0 intermediation activities, the BGH found that an Internet portal on which end-users could publish their own content (in this instance, food recipes) was civilly liable, in a situation where the portal (as was the case) reviewed the content before publishing it, and thus, in some manner or form, "appropriated" it. The BHG deemed that, as a result of this process of appropriation, there was a direct infringement of copyright, compounded by the fact that the portal displayed the content under its own logotype for gain.[170]

In a similar case, however, the decision of the Hamburg OLG of 29.9.10[171] (*Sevenload* case) found that there had been no "appropriation" of content generated by the end-users, due the fact that said content had not been subjected to prior examination, even though an editorial structure had been furnished to render online publication possible. In view of the fact that there was no direct infringement in this case, the Hamburg OLG went on to analyse the Web 2.0 platform operator's possible liability by way of *Störerhaftung,* a possibility that was likewise dismissed due to its being unable to carry out *a priori* control of the material uploaded to the network by the end-users. Only where specific notification was received to the effect that given material infringed third-party rights did a duty arise to block content and prevent similar infringements.

Lastly, the Hamburg OLG's decision of 24.7.2008[172] held that an online auction portal was liable for direct trademark infringement of counterfeit products sold on the portal.

b) *Hyperlinks to illegal content matter*

With respect to liability for the establishment of individual hyperlinks to illegal content matter, the BGH's decision of 20.10.2010[173] (*AnyDVD* case) concluded that the establishment of a hyperlink on a web page, which then conveyed the user to another page where instruction was given on how to deactivate the technological protection of DVDs, did not constitute an act of circumvention of technological measures under Article 95 of the CA (a provision based on Article 6 of the Directive 200/29/CE). The Court deemed that the establishment of individual hyperlinks was covered by the freedom of the press and information under §5 (1) of the German Constitution, a decision that was subsequently confirmed by the German Constitutional Court in its

[168] GRUR 2007, p. 890 ff., case of *Jugendgefärhdende Medien bei Ebay*, available at website address <http://medien-internet-und-recht.de/volltext.php?mir_dok_id=1349>.
[169] GRUR 2010, p. 616 ff. and *Multimedia und Recht*, 2010, p. 556 ff., available on the Internet at <http://medien-internet-und-recht.de/volltext.php?mir_dok_id=2181>.
[170] The Court held that, for this purpose, the mere declaration by the user that the content did not infringe third-party rights could not suffice to free the provider of liability; and the same could be said of the licence obtained by the ISP to exploit content. On the contrary, it was evidence of the fact that the ISP was seeking in this way to take advantage of users' content as though it were its own.
[171] *Multimedia und Recht*, 2011, pp. 49-51, available on the Internet at <http://medien-internet-und-recht.de/pdf/VT-MIR-2010-Dok-162.pdf>.
[172] *Multimedia und Recht,* 2009, pp. 129 ff., available at <http://openjur.de/u/30706.html>.
[173] Available at <http://openjur.de/u/163878.html>.

decision of 15.12.2011.[174] In a similar case, the BGH's decision of 17.7.2003[175] (*Paperboy* case) held that provision of hyperlinks to content that infringed intellectual property rights was not an instance of direct copyright infringement by reproduction of a work.

Additionally, the BGH has stated that the exemption of hosting providers under §10 of the TMA[176] is not applicable to the provision of hyperlinks to illegal content, due to the fact that the latter do not constitute an intermediation service such as those envisaged under the Act, and that in this case the general rules of co-participation in infringing activity for civil actions for compensation and possible criminal liability were applicable.

In the criminal field, a number of guilty verdicts have been pronounced by District Courts (LG) on Internet portal operators who supply thousands of hyperlinks to content that violates intellectual property rights. This was the case, for example, of the decision of the *Leipzig LG* of 11.4.2012, which sentenced one of the main programmers of the *Kino.to* hyperlink portal to a prison sentence of just under four years.[177]

c) *Internet search engines*

In Germany, the matter of the civil liability of Internet search-engine operators has basically been settled by two Supreme Court decisions. The first of these judgements was rendered on 29.04.2010[178] in the *Vorschaubilder* case,[179] in which an artist who exhibited digital copies of his/her works on a personal web page brought an action against *Google* for the *Google Images* service, which indexes pages and displays a small-scale reproduction of the images -known as "thumbnails"- in its search results, when the appropriate key word (the artist's name for example) is entered.

The BGH held that, though there had been acts of reproduction[180] and communication to the public[181] on the part of the Defendant, no liability whatsoever could be attributed to the search-engine operator because the author of the images, on having included them in a web page without technical protection against the indexing activity of search-engine operators, was tacitly or implicitly consenting[182] to said indexing and display of search results vis-à-vis third parties.[183]

---

[174] The text of the German Constitutional Court's decision is available at <http://www.bundesverfassungsgericht.de/entscheidungen/rk20111215_1bvr124811.html?Suchbegriff=1+BvR+1248%2F11>.

[175] Available on the Internet at <http://www.jurpc.de/rechtspr/20030274.htm>.

[176] *GRUR 2008*, pp. 534, case of *ueber18.de* and *GRUR 2004*, pp. 693, case of *Schoener Wetten*.

[177] The press report of the decision can be seen at <http://www.jurablogs.com/thema/landgericht-leipzig>.

[178] The decision is available, with an introduction in English by Philip ZIMBEHL, at 3 (2010), *JIPITEC*, p. 190 ff., and at <http://www.jipitec.eu/issues/jipitec-1-3-2010/2798>.

[179] Available in German at <http://medien-internet-und-recht.de/volltext.php?mir_dok_id=2177>.

[180] In reality, as was analysed on reviewing the *Google Images* judgements in France, it is debatable to maintain that the images shown on the *Google Images* service are reproduced on the search engine operator's server. This is because, even though the end-user has the impression that the images shown "are" on the search-engine servers, this is not so from a technological point of view: it is a mere visual impression (each image continues to be stored on its "original" server).

[181] The BHG held that the storage of the images on the *Google* servers constituted an act of reproduction under §16 of the Copyright Act, which should in principle be authorised by the owner of the rights. Nevertheless, insofar as the reproduction was stored on *Google* servers located in the United States, the principle of territoriality barred the application of the German Copyright Act in this case.
The decision also held that the search engine operator undertook an act of public communication pursuant to §19a of the Copyright Act, and that the limits or exceptions for quotations (§51 of the Act) or the limit for certain acts of transient or accessory reproduction envisaged under Article 5.1 of the Directive 2001/29/CE and implemented in Germany by §44a of the Copyright Act were not applicable to the case before the court.

[182] The BGH deemed that, in line with the principle of *bona fide* and the functioning of the network itself, tacit consent to being indexed by search engines was given when the images were inserted into a

The BGH also held (though only by way of *obiter dicta*) that, even if such individual tacit authorisation had not existed, the search-engine operator could have benefited in this instance from the exemption from liability envisaged under Article 14 of the DEC, since it was undertaking an activity that was of a merely technical, passive and automatic nature, and thus had no control over the indexed material nor any prior effective knowledge of its being unlawful, citing the CJEU's decision in the *Google France* case.

This doctrine has been repeated by a second decision issued by the BGH itself on 19.11.2011 (the *Vorschaubilder II* case),[184] in which it again held that the search-engine operator should not be held liable for acts of reproduction or communication of thumbnail images shown on the *Google Images* service, having recourse to the idea of tacit consent by photographers -the holders of the rights in the snapshots- who had assigned the rights to exhibit the photographs on two websites from which the *Google* robot had retrieved the images.

The fundamental novelty in relation to the *Vorschaubilder I* decision is that here the BGH now deemed the doctrine of implicit consent to be equally valid when it was a third party that commercially exploited the content matter without the rightholder's permission.[185] In particular, the BGH stated that it was a well-known fact that search-engine operators drew no distinctions when it came to the matter of whether material was uploaded to the Internet with or without the owner's consent, and sounded a reminder to the effect that, in any event, recourse could still be had to the action against the website which originally performed the unlawful act of reproduction and public communication.

d) *Distributors of file-exchange programmes*

With reference to persons who design and distribute Internet programmes to enable end-users to exchange files over P2P networks, the Hamburg OLG's decision of 6.2.2006[186] ruled that the placing on the Internet of a computer programme (*Cybersky TV*) which enabled users to "stream" different TV programmes owned by the Claimant (a coded television broadcasting corporation) was in breach of the German Unfair Trade Act, and ordered a total halt to be put to the infringing conduct.

The OLG held that in order for there to be an infringement of the related rights of the broadcasting corporation (§87 (1) (1) of the German Act), it was not necessary that the signal be emitted directly. It sufficed that there was a direct causal connection with the conduct of the infringers (end-users), a connection which in this case existed, owing to the fact that, beyond the formality of some disclaimers, no measure had been introduced by the software developers to prevent the programme from being used to retransmit coded television signals. In the OLG's view, such liability did not so much arise from the infringements that had already taken place, but rather from those that

---

proprietary web page without protection against the search engines, and that individualised notification to *Google* did not suffice to revoke such consent. This revocation would have to be targeted, not at a single intermediary, but at the general public, and would have to be achieved by means of a simple technological mechanism that instructed the search engine operators to exclude the content from the results yielded by the robot. It is the use of this simple "anti-search engine" mechanism which indicates that the rightholder is revoking the consent that he/she tacitly gave when posting the content online.

[183] The BGH moreover defined the difference between this tacitly given consent and a genuine licence. Whereas consent solely serves to justify an infringement of the right in a specific case, a licence, on the other hand, is a contractual authorisation that permits the commercial exploitation of the work.

[184] Available at <http://medien-internet-und-recht.de/pdf/VT-MIR-2012-Dok-016.pdf>.

[185] In the case of a licence to make use of the images reproduced by *Google*, this had been granted for a web page other than that used by the robot to make the thumbnail images (a page that was thus illegally exploiting the works).

[186] See the summary of and commentary on the case in RÖSLER, H., *IIC* 8/2006, pp. 989 to 997.

would potentially result from putting on the market a product of these characteristics without incorporating into it any type of mechanism designed to prevent customers who used it from infringing third-party copyright[187]

Subsequently, the BGH's judgement of 15.1.2009[188] confirmed the OLG's decision, by banning the offer, operation or distribution of the P2P application while it continued to allow the transmission or reception over the Internet of the decrypted signal owned by the broadcasting corporation.

IX. ITALY

1. Legislation

In Italy, the statute incorporating the DEC into the national law was passed by Decree-Act No. 70/2003 of 9 April 2003.[189] This Decree follows the approach of the Directive very closely,[190] creating a special regime of limited liability for ISPs, one that partially amends the provisions laid down in the Civil Code by Articles 2.055 (joint and several liability in a case where the unlawful act is committed by several persons) and 2.049 (culpable liability, on failure to implement the pertinent controls that could have prevented the commission of the unlawful act).

Article 14 of the Decree-Act establishes a limitation of liability for ISPs who undertake mere conduit activities, with a literal tenor which is almost identical to that of Article 12 of the Directive. It thus provides that the information must be furnished by a third party (not by the ISP itself), that the ISP must not select the receiver of the transmission, and that the ISP must neither select nor modify the information transmitted.[191]

Article 15 contains the safe harbour for proxy caching activities, establishing for the purpose a series of conditions similar to those envisaged under Article 13 of the DEC (i.e., the provider must not modify the information, must comply with conditions on access to the information established by the party supplying same, and must comply with rules regarding the updating of the information, specified in a manner widely recognised and used by industry, etc.).

---

[187], Following a number of contradictory judgements in the Regional Appeal Courts, the German Supreme Court in its decision of 12 May 2010 finally ruled that any user whose connection had been used to carry out these types of acts was subject to interlocutory actions or interim injunctions. Nevertheless, if the user were blameless (as occurred in this case, in which it was shown that the allegedly infringing user was on holiday when his/her wi-fi connection was hacked by a third party and used for the exchange of files), he/she could not be made the subject of an action for compensation. See the decision at <http://medien-internet-und-recht.de/volltext.php?mir_dok_id=2182>.

[188] *GRUR 2009*, p. 841, available on the Internet at <http://medien-internet-und-recht.de/pdf/VT_MIR_2009_155.pdf>.

[189] *Gazzetta Ufficiale* No. 87 of 14 April 2003.

[190] The Bill of 26 July 2011 sought to amend the regulation contained in Article 16 of the 2003 Legislative Decree requiring access providers to disable access or remove content in the event of there being notification by any "interested party" and not only by the judicial authorities, as is currently the case. The Bill did not however survive the parliamentary stage (the text thereof is available at website address <http://www.camera.it/>). Subsequently, an attempt was made to introduce its content into the so-called "Fava amendment", adding an amendment to the 2011 Community Act (C 4623 *Governo*) intended to append a new Article 5 to the Act, which was also rejected during its passage through Parliament (the text of the amendment is available at <http://www.leggioggi.it/allegati/legge-comunitaria-2011-emendamenti-e-articoli-aggiunti-in-sede-desame-dalla-camera-dei-deputati/>).

[191] Article 14.2, in much the same way as Article 12.2 of the DEC, addresses the specific case of transient and technical reproductions, whilst Article 14.3 makes use of the power vested in the national legislature by the Directive to establish interim measures and actions for injunction in respect of network operators and access providers (Article 14.3), proxy caching activities (Article 15.2) and hosting activities (Article 16.3), provided, in all cases, that these are ordered by the competent judicial or administrative authority, regardless of the outcome of the action for compensation.

Article 16 of the Decree regulates hosting activities, making exemption from liability conditional on the fact that the hosting service provider has no actual knowledge that the activity or information is illegal (a reference to *mens rea* as a subjective requirement in the criminal field) or (in the case of a civil action for compensation) that it is unaware of facts or circumstances which make the illegality of the act or information apparent (and which must be taken to refer to culpable or negligent conduct).[192]

The hosting service provider will also remain outside the safe harbour if it fails to disable access to the information or remove it from the network *as soon as* it obtains knowledge, through notification from the competent authority, of facts that reveal the illegal nature of such information (Article 16.1 b) of the Decree-Act). Beyond this general reference to the "competent authority", the Decree envisages no formal procedures for the detection and removal of material.

Lastly, Article 17.1 excludes the general obligation to monitor content, making it clear that ISPs have no duty to carry out any active investigation into facts or circumstances that may indicate the presence of an illegal activity. Nevertheless, in any case where the provider may know of allegedly illegal activity or information concerning the end-users of its services, it is required to collaborate with and inform the judicial and administrative authorities, something that includes an obligation to supply these same authorities with such information as will enable the recipient of the service with whom there is the contractual tie, to be identified for the purpose of *locating* and *preventing* said illegal activity (Articles 17.2 a) and b) of the Decree).

Furthermore, Article 17.3 states that any ISP who fails to act promptly to bar access to the material following a request from a competent administrative or judicial authority in the course of its monitoring duties, will be held civilly liable.[193]

Aside from this Decree-Act dating from 2003, which incorporates the DEC into Italian national law, the Italian legislature has specifically attempted to cut short the phenomenon of P2P networks by a Decree-Act of 12.3.2004. This enactment amended Article 171-*ter* of the Copyright Act of 22 April 1941 to include, as administrative misconduct (and thus penalised by a fine), the use of information and communications technology to dissemination copyright-protected cinematographic or like works, or any part thereof, to the public, via networks or connections of any type, including file-exchange programmes. Very shortly afterwards, the statute converting said Decree (Act No. 128 of 21 May 2004)[194] changed the system again, by replacing the administrative penalties applied to users with a system fundamentally based on criminal sentences.[195]

In Italy, moreover, there has been an initiative for a new regulatory scheme. This has come from the Communications Guarantee Authority (*Autoritá por la Garanzie nelle*

[192] As also envisaged under the Directive, the exemption is not applicable if the recipient of the service acts under the direction or control of the ISP.
[193] The ISP will also be answerable in any case where, having had knowledge of the illegal or prejudicial nature of the content thanks to a third party to which access is provided (e.g., another of its subscribers), it has then failed to inform the competent authority of said illegal nature.
[194] Available at website address <http://www.camera.it/parlam/leggi/04128l.htm>.
[195] Hence, the Act of 22 April 1941 was firstly amended throughout, by replacing the term, "with a profit motive" (*a fini di lucro*), with the broader term, "to obtain a profit" (*per trarne profitto*). Secondly, subsection a)*bis* was added to Article 171-ter.2 of the 1941 Act by way of a new form of offence punishable by a prison sentence of one to four years in the case of any person who, "*in breach of Article 16, and for gain, communicates to the public, by introducing into a networked information and communications system, by connections or by any other means, a copyright protected work or any part thereof.*"

Comunicazione AGCOM), which by Resolution No. 398/11/CONS of 6.7.2011[196] proposed a new body of rules that would allow for the intervention of this administrative authority in cases involving copyright infringement on digital networks, by means of a notice and take down process with counter-notification.[197] However, this initiative has recently been dropped.[198]

2. Case-law

a) *ISP liability*

One of the first Italian judicial decisions on ISPs was that in the *Peppermint* case, in which the ruling issued by Civil Section 9 of the Rome Court on 16.7.2007 dismissed the plea filed by the record company of the same name to identify 3,600 end-users who were using the services of an ISP to exchange files over P2P networks.[199]

Subsequently, the Rome Civil Court's decision of 15.4.2010[200] in the case of *Federazione Antipirateria Audiovisiva (FAPAV) v. Telecom Italia* held that the access provider was not to be held answerable for information transmitted by the end-users of different web pages that furnished *torrent* hyperlinks for peer-to-peer applications (including some of the best known ones, such as *The Pirate Bay* and *isoHunt*) and, in addition, rejected the request to have said web pages blocked. The court did, however, order the ISP to supply the Public Prosecutor's Office with the notifications of infringement received from the various rightholders.

Recently, however, the Cagliari Public Prosecutor's Office ordered the *Guardia de Finanzas* [an Italian law enforcement agency somewhat similar to the Duty & Excise Department] to interrupt or block Italian end-users' access to the torrent download site, *www.BtJunkie.org*, on the basis of Article 14 of Decree-Act 70/2003, which, as has been seen, requires ISPs to obey the orders of the judicial authorities (as a matter of urgency if needs be) to prevent or bring a halt to infringement of intellectual property rights.[201]

b) *Web 2.0 intermediation activities*

In the case of Web 2.0 platform operators, Italian case-law has generally shown itself to be in favour of not applying the privileged liability regime contained in Decree-Act 70/2003,[202] rendering said operators liable in cases of infringement committed on their

---

[196] Official Gazette No. 163, of 15 July 2011, available at <http://www.agcom.it/default.aspx?message=visualizzadocument&DocID=6693>.

[197] Said action is fundamentally based: on Article 182 b of the Copyright Act (added into the Copyright Act 633/41 by Act 245/2000), which vests the *AGCOM* with monitoring powers regarding, among other things, observance of copyright in acts of reproduction by any means, in the audiovisual sphere, by radio or television; and on Article 32-b of the Legislative Decree 44/2010, which requires communication service providers to respect intellectual property rights, and confers on the *AGCOM* a general power of inspection and the capacity to issue regulatory provisions to implement the goals pursued by this Legislative Decree.

[198] This is to be understood from the declarations made by the Chairman of same before the Italian Senate, available at <http://www.nuovoimaie.it/it/news/in-primo-piano/sconcerto-e-delusione-di-nuovo-imaie-per-il-dietrofront-di-agcom.html>.

[199] An explanation of the case is available in AGCOM Judgement No. 398/11/CONS of 6 July 2011, p. 13.

[200] RG 81287/09, summary available at <http://www.downloadblog.it/post/11645/fapav-e-p2p-attesa-sentenza-court-di-roma>.

[201] See the reference to the case on the Internet web page <http://blog.dlapiper.com/iptitaly/entry/injunction_for_btjunkie_org>.

[202] A criminal sentence has also been handed down for breach of privacy and data-protection laws in a case where a video, in which a disabled student was being harassed by his/her classmates, was uploaded to an audiovisual exchange platform and remained available online for over two months. See the decision of the Milan Lower Court (*Tribunale Ordinario*) of 24 February 2010, No. 1972/2010, available at <http://www.giurcost.org/casi_scelti/Google.pdf>.

platforms, if they fail to fulfil their monitoring obligations in respect of content already recognised or notified as being infringing.

Hence, in the case of *Reti Televisive Italiane v. YouTube* (writ of court issued by the Rome Court on 15.12.2009),[203] the Court concluded that video exchange platforms had to accept a stricter standard of liability than that provided for by Article 14 of the DEC, requiring the intermediary to seek and remove from its service all content matter owned by the Claimant.

In much the same vein, the Milan Court's decision of 19.5.2011 in the case of *RTI Italia v. Yahoo Italia SRL*[204] ruled that the safe harbour for hosting activities envisaged under Article 16 of the Decree-Act 70/2003 could not be applied to the activity undertaken by the Defendant (a video exchange platform), since the latter had assumed an active role in the organisation and management of the platform,[205] something for which, moreover, the company obtained a financial benefit.[206] Accordingly, the Court held that, even though there was no general obligation to carry out prior monitoring, content had to be removed in any case where an owner identified an URL on which infringing material was hosted.

In its decision of 20.10.2011,[207] the Rome Court sounded a similar note in an action that once again brought *RTI Italia* up against the provider of access to and hosting of a website via which end-users could exchange videos that included complete episodes of at least three television series whose rights corresponded to the Claimants.

The Rome Court held that a service provider's possibility of benefiting from the exemption from liability envisaged under Article 14 of the Directive depended on its active or passive role, stating that in this particular case its conduct had been restricted to making space available to a third party so that the latter could set up a file-exchange website. In this case, therefore, the Court deemed that the ISP would only be answerable if it had received detailed notification *by the competent administrative or judicial authority* (not from the owners) with respect to each and every infringing item, and had not acted diligently to remove or disable access to same.[208]

Lastly, it should be noted that the Milan Court writ of 20.1.2011[209] (*RTI v. IOL)* ruled that the operator of an electronic platform on which end-users were allowed to up- and download protected broadcasted material was to be deemed a direct infringer of intellectual property rights.

The Court underscored the active nature of the website operator in the design and management of the file-exchange platform (key-word search, indexing of videos, etc.) and the financial benefit that it obtained, thanks to the presence of hyperlinks inserted

[203] No. 54218/2008, available at website address <http://www.tgcom24.mediaset.it/res/doc/sentenzacourt.pdf>.
[204] The decision is available at website address <http://www.leggioggi.it/wp-content/uploads/2011/09/sentenza_mediaset_yahoo.pdf>.
[205] The court held relevant activities to be the establishment of a key-word search service for videos, the task of indexing and offering videos similar to that which a user was viewing at any given time, and the offering of a mechanism whereby the platform operator reviewed any video reported by users to be infringing and proceeded to remove it where deemed appropriate.
[206] Published on 15 September 2011, case summary and commentary by BARBIERI, A., and DE SANTIS, F., available at <http://www.portolano.it/wp-content/uploads/2011/10/Protection-of-television-programmes-on-video-sharing-platforms-06.10.11.pdf>.
[207] Available at <http://www.comellini.it/autore_file/ordTribRoma.htm>.
[208] Moreover, the Court found the other co-defendant, the website owner, guilty as a direct infringer of copyright.
[209] The decision is available at <http://www.leggioggi.it/wp-content/uploads/2011/11/Trib.-Milano-7_6_2011.pdf>.

by third-party advertisers associated with the videos exhibited. In addition, there was the fact (which appeared to be decisive in the case) that the Claimant broadcasting corporation had sent a request to IOL to cease its activity, which received no response.

c) *Link-listing websites*

In the case of web pages which supply hyperlinks to digital storage facilities or which launch applications to enable end-users to download files over P2P networks, the decision handed down by Criminal Section 3 of the Italian Court of Cassation on 23.12 2009[210] (*Pirate Bay Italia* case) ruled that the order of a Bergamo Lower Court mandating the blocking of the site for Italian end-users was good in law, despite the fact that the order had been set aside on appeal.

d) *Internet search engines*

In the case of *PFA Films S.r.l. v. Google Italy, Microsoft S.r.l. and Yahoo! Italia S.r.l.*, (court order of the Rome Court of 20.3.2011),[211] the Court ordered the search-engine operator *Yahoo!* to remove from its servers all hyperlinks to websites which offered illegal copies of the motion picture "*About Elly*". The Court held that, even though search-engine operators may not be bound to carry out prior monitoring of the content to which they provide links (Article 15 of the DEC), they are nevertheless required to act by removing hyperlinks to illegal content upon obtaining knowledge of such illegality (applying Article 14 of the DEC by analogy).

Given that the search-engine operator in this case had been informed of the illegality of the material by the rightholders, it was to be deemed a "joint infringer" for the purposes of being a recipient of the interim injunction (for cessation) envisaged under copyright legislation. The Court thus allowed that there had been collaboration in the infringement on the part of the search-engine operator, but confined itself to admitting the action for injunction to remove the hyperlinks, without ordering any sum to be paid by way of compensation.

X. MEXICO

The civil and criminal liability of Internet intermediaries in Mexico is regulated by the rules of the *jus commune*, as there is still no special legislation governing the matter.[212]

A Bill to amend the Federal Copyright Act (FCA) of 15 December 2011[213] is currently under way, however, and this is sought to be used to regulate the issue of online rights infringement.
Insofar as ISPs are concerned, the Bill (which is not the first[214] in Mexico)[215] seeks to amend Article 231 (sections 3 and 10) of the FCA in order to render making content

[210] The decision is available at website address <http://www.altalex.com/index.php?idnot=48812>.
[211] Available at <http://www.blogstudiolegalefinocchiaro.it/wp-content/uploads/2011/03/Ordinanza_PFA-Yahoo.pdf>.
[212] Indeed, in contrast to other Latin American countries, such as Chile or Colombia, which have concluded bilateral agreements with the United States that require them to implement rules on ISPs in their national legislation, Mexico has a regional agreement in the form of the North American Free-Trade Agreement (NAFTA), which links it to the USA and Canada, and which, in its provisions on protection of intellectual property, does not include specific rules on exemptions from liability of ISPs, on having entered into force before this question arose at an international level (the treaty came into force on 1 January 1994).
[213] This is the *Proyecto de Decreto que reforma la ley Federal del Derecho de Autor y adiciona un capítulo y diversos artículos a la Ley de Propiedad Intelectual* (Senate Gazette of 15 December 2011), known in the Mexican mass media as the "Döring Act", on being named after Federico Döring Casar, the Senator who first tabled the Bill. The Bill is available on the Mexican Senator's web page, and is accessible at website address <http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=12788&lg=61>.

available on the Internet *by any means and in any format* (e.g., via P2P networks) a commercial offence, even in a case where this not for profit and there is no prejudice to a third party. The Bill also proposes the addition of Articles 202*bis* to 202*bis* 6 of the Industrial Property Act to create an Internet notification procedure with respect to infringements that run counter to the normal exploitation of a work.[216]

To the extent that, at the time of writing this study, the future of said Bill was still uncertain, the rules to be applied to elucidate the liability of intermediaries who collaborate in online infringement of intellectual property rights are, as stated above, those of the *jus commune*, together with those of the 1996 WIPO Treaties which Mexico has ratified (and Article 8 of the WCT, in particular).

In the civil sphere, the benchmark law is the 1996 FCA,[217] which does not, however, contain special rules for attributing civil liability to joint infringers of copyright and related rights, on setting forth the civil (Article 213 of the FCA) and administrative defence mechanisms (Article 229 of the FCA). Neither does it contain specific rules with respect to actions for injunctions, despite the fact that Mexico is a party to the Trade-Related Aspects of Intellectual Property Rights (TRIPS) Agreements.

Based on the principle of *neminen laedere* of Article 1.910 of the Mexican Civil Code, the general rules of non-contractual civil liability are thus applicable. Consequently the problems that have arisen in other Latin American countries when seeking to determine the precise degree of causal connection between intermediaries and unlawful conduct are reproduced in Mexico, due to the absence of a general theory of liability for contribution to infringing acts or secondary liability, which is well defined in the British and American Common Law systems.

The lack of specific legislation coupled with disagreement as to how to go about regulating the issue have resulted in an absence of civil court claims, with respect both to ISPs in the strict sense (access, proxy caching and hosting providers) and to operators of Web 2.0 electronic platforms that are used by end-users to exchange illegal content matter, though there have indeed been numerous IMPI-led administrative procedures (IMPI: *Instituto Mexicano de Propiedad Intelectual*) to delete Internet web pages from which copyright-infringing files were being offered.

In the criminal field, as regards the rules governing situations where there are two or more persons responsible for a criminal act, the statutory provision applicable would be

---

[214] There has also been a *Proyecto de Decreto por el que se adicionan y modifican diversas disposiciones de la Ley Federal del Derecho de Autor* modelled on the French HADOPI Act, though with a double warning system (Parliamentary Gazette of 27 April 2010), available at <http://gaceta.diputados.gob.mx/Gaceta/61/2010/abr/20100427-X.html)>.

[215] Another unsuccessful Bill, the *Proyecto de Ley Federal para la Protección de los derechos de los usuarios de Internet de 2 de abril de 2009*, was also proposed, which envisaged including new limits for exclusive rights in digital environments, including a limit that enabled temporary copies of content to be made in the RAM memory of PCs (e.g., while screening online content in streaming mode). The Bill also barred ISPs from halting the access service without an express court order (Article 8). See the text at <http://www.senado.gob.mx/index.php?ver=sp&mn=2&sm=2&id=13010&lg=60>.

[216] The proposed law empowers the Mexican Intellectual Property Institute (MIPI) to notify Internet users who commit an infringement against the normal exploitation of the work, and to initiate the procedure *ex officio* or at the request of the interested party. Additionally, the MIPI can, subject to a prior request from the aggrieved rightholder, ask ISPs to provide it with the identity of the user who used the IP address from which the allegedly infringing conduct was carried out. Once identified and duly notified, the user then has a period of 3 days to submit such pleadings as he/she deem suitable, after which the MIPI will decide in accordance with the Act.

[217] The Act implements Article 28 of the Mexican Constitution, which protects authors and artists from the anti-monopoly rules by means of temporary privileges granted to them under the Act for commercial exploitation of their works. There is a version of the Act in English, updated to January 2012, available at <http://www.wipo.int/wipolex/es/details.jsp?id=11495>.

Article 13 of the Federal Penal Code, which lays down the general rules of responsibility and complicity for attributing criminal liability to, among others, accomplices who *wilfully* aid or abet another in the commission of an offence (Article 13. VI, of the Penal Code). Liability also exists in cases where, without prior agreement, there is joint action in the consummation of an offence and the outcome ascribable to each of the participants cannot be precisely ascertained (Article 13 VIII of the Penal Code).

In the absence of special criminal legislation on the matter, however, there are evident difficulties in the way of the courts deciding to apply the pertinent rules to cases involving Internet intermediaries, where collaboration with infringement is normally secondary and the requirement of *mens rea* is hard to prove.

This is exacerbated by the fact that Article 424*bis* of the Penal Code requires a profit motive for the basic type of offence against intellectual property, something that further complicates the task of determining liability for collaboration in cases such as the exchange of files over P2P networks and Internet pages that supply hyperlinks to end-users for the purpose, since the figure of the principal infringer is "missing", even in cases in which it is clear that the accessory or accomplice does indeed have the necessary profit motive. This could be one of the reasons that would account for the absence of criminal decisions in Mexico with respect to this question.

XI. MOROCCO

In the field of copyright, the law in force in Morocco is the Copyright and Related Rights Act No. 2-00[218] (CRRA), promulgated by *Dahir* No. 1-00-20 of 9 *Kaada* 1420 (15.2.2000).

This Act envisages a generalised protection for copyright and related rights through the attribution of ownership (Article 10) and moral rights (Article 9), and affords protection to performers (Article 50), producers of phonograms (Article 51) and broadcasting corporations (Article 52), with a range of statutory actions for the protection of these rights, including interim (precautionary) measures under Article 61, civil actions for injunction and compensation (under Article 62), and criminal actions under Article 64 of the Act and Articles 575 to 579 of the Penal Code.[219]

With regard to intermediary's liability for infringement of intellectual property rights,[220] the statutory provision applicable is *Chapter IVbis* of Act 2-00, in conjunction with Act No. 34-05 which implemented into the country's internal law the Free-Trade Agreement (FTA) between the United States and Morocco, a treaty that contains a regulation of ISP liability modelled on Article 15.11 of the US Digital Millennium Copyright Act.[221]

Article 65.3 of Act 2-00 thus contains a definition of service provider, which describes the usual activities in such cases, including the mere provision of access and transmission of information.

---

[218] The Act is available at <http://www.wipo.int/wipolex/es/details.jsp?id=2985>.

[219] According to the doctrine, in the criminal field the general rules of participation in an offence will apply to the case of aiding or abetting an infringement. On this aspect see HIDASS, A., *Le droit d'auteur au Maroc*, UNESCO Copyright Bulletin, Vol.XXXV No. 2, April-June 2001, UNESCO Editions, p. 80.

[220] A regime of exemption from "horizontal" liability is thus not established for all types of illegal content, but only for violations of copyright and related rights committed by the end-users of these types of services.

[221] Specifically at Clause 28, under the head, "Limitations on service providers' liability".

Based on this definition, the technique followed by the Moroccan legislature has been to define the general rules or criteria for attributing liability to ISPs in Article 65.4 of the Act, and then go on to establish a list of exemptions from said liability or safe harbours in Article 65.5.

Hence, Article 65.4 (A) lays down a general principle of liability for contribution to the offence, on stating that any service provider who knows or has reasonable grounds to know of any infringement of intellectual property rights (copyright and related rights) committed by another person shall be held civilly liable, if it should *encourage*, cause or *substantially contribute* to such illegal activity.

There is also criminal liability for contributing to infringing acts -Article 65.4 (B)- in the case of any ISP who wilfully causes damage, or encourages or substantially contributes to the infringement of intellectual property rights committed by another person.

Article 65.4 (C) establishes the principle of civil liability for ISPs with respect to third-party acts (vicarious liability), albeit with the requirements: that the provider have the right and capacity to monitor or control rights violations committed by other persons; and that it directly obtain a financial interest from the unlawful activity, which will not be frequent in practice.

Lastly, Article 65.4 (D) of the Act establishes criminal liability for a willing accessory or accomplice, in any case where one party wilfully monitors or controls an infringement of rights committed by another and there is a direct financial interest in the activity. These will thus be cases in which it is difficult to speak of a task of pure intermediation, with the publisher and intermediary having acted of one accord.

In all the above-mentioned cases, actions -civil or criminal- can be brought directly against the ISP, without simultaneously having to file a lawsuit against the infringing end-user (Article 65.4 (E) of the Act).

Insofar as regulation of ISP safe harbours is concerned, Article 65.5 of the Act contains the general principle of exemption from liability in accordance with the conditions laid down in Articles 65.12 to 65.14, provided that the requirements stipulated by the Act in Articles 6.6 to 6-11 are met.

To this end, Article 65.5 subsections A to D classify intermediation activities into four categories, which are similar to those in the DMCA and differentiate between activities of mere transmission and provision of network access,[222] provision of system caching services,[223] hosting of information provided by a recipient of the service,[224] and the use of Internet search services or engines or the establishment of hyperlinks to content matter supplied by third parties.[225]

In the specific case of network transmission system providers and network access providers under Article 65.5 (A), these ISPs have no specific condition assigned for being eligible to benefit from the exemption: for the limitation of liability to be applied to them, it thus suffices to show that they carry out mere conduit activities and fulfil the general requirements of Articles 65.4, 65.6 and 65.10.[226]

[222] Article 65.5 (A) of the Act.
[223] Article 65.5 (B) of the Act.
[224] Article 65.5 (C) of the Act.
[225] Article 65.5 (D) of the Act.
[226] Lastly, it should be pointed out that Article 13 contains a limit to the right of reproduction in order to permit the making of provisional reproductions, similar to that provided for by Article 5.1 of Directive

Article 65.8 lays down the conditions to be met by ISPs to be entitled to benefit from the limitation of liability for activities of automatic storage of content (proxy caching), requiring them, as is standard in such cases, to permit the updating or reloading envisaged by the content's owner, and not to tamper with the measures used to count visits to the original page [i.e., the so-called "hits"], etc.

Article 65.9 sets out common conditions for hosting service providers and owners of online search and/or hyperlink provision services, requiring that there be no profit directly attributable to the activity which leads to the infringement of intellectual property rights if the provider has the capacity to monitor or control said activity,[227] that the provider act promptly to remove or disable access to content upon obtaining actual knowledge of the illegality thereof (and said knowledge is obtained in any case where notification has been received pursuant to the notice and take down process under Article 6.13),[228] and that it have a public representative to whom such notifications may be sent.[229]

There are, moreover, some common conditions for the four types of intermediation activities defined by the Act. Hence, Article 65-6 provides that the exemptions from liability are only applicable to intermediaries who select neither the content matter nor those receiving it, save in the case of search engines and provision of hyperlinks, in which, as Article 65.6 of the Act itself states, a form of selection is intrinsically present. Another common condition for all four intermediation activities is likewise established by Article 65.10 of the Act, which requires ISPs to have certain general conditions for terminating the contracts of infringing end-users, and not to interfere with the use of any technological protection and information measures for digital management of intellectual property rights which have been agreed upon by the owners and the ISPs themselves.

Lastly, Article 65.11 lays down that application of the limitations of liability does not depend on whether the ISP undertakes active surveillance or monitoring of its systems to find facts or evidence of infringement of copyright and related rights. Furthermore, Article 6.15 makes it obligatory for ISPs to collaborate with the Moroccan National Copyright Office for the purpose of identifying end-users who post allegedly infringing material online.

The specific scope of the limitation of liability is outlined in Articles 65-12 to 65-14 of the CRRA. Article 65.12 states that, even in a case where application of the safe harbour is in order, actions for injunctions for mere conduit activities remain unaffected, so that the court may order the suspension of a specific end-user account or the disablement of infringing websites located abroad.

In the case of activities of proxy caching, hosting, and provision of online search and hyperlink services, the court s also empowered to order the removal of or disablement

---

2001/29/CE, which requires: that the reproduction take place during the digital transmission of a work or act leading to the display of digitally stored work (browsing); that said copy be made by a natural person or legal entity authorised, by the copyright owner or by the law, to carry out said transmission of the work or act designed to make it perceptible; and, lastly, that the reproduction be of an accessory nature, take place during normal use of the material and be deleted automatically, without any act of utilisation of the work for purposes other than those specified in subsections a) and b) being permitted. This provision may be used to exempt from liability acts of transient storage undertaken during the digital transmission of works (in a manner similar to Article 12.2 of the DEC), thus protecting enterprises which conduct activities of mere transmission (mere conduit).

[227] Article 65.9 a) of the Act.

[228] Article 65.9 b) of the Act.

[229] Article 65.9 c) of the Act.

of access to the infringing material, provided that such measures prove less invasive for the ISP than others that might have a similar effect.

Article 65.13, contains a detailed notice and take down process, which must be followed in order to be entitled to benefit from the exemption from liability in proxy caching, hosting, and provision of online search and hyperlink services. This statutory provision lists the requirements and minimum content which such notification must have (adequate identification of the owners, protected literary and artistic works affected, and infringing materials, etc.). In the case of search engines or hyperlink pages, it is necessary to furnish some means that enables the hyperlink to be reasonably identified, and, if the notification refers to a considerable number of hyperlinks on a single page, the provision of a representative list and web page address will suffice.

Finally, Article 65.14 establishes the general legal regime for limitation of liability for intermediaries who remove or disable access to any content which, in good faith, they deem to be unlawful in view of the notification request received from the owners. In order to be able to benefit from this exemption, the ISP[230] must immediately advise the content's owner, because, if the owner of the allegedly infringing material should serve a counter-notification in accordance with the rules stipulated for the purpose in Article 65.14 C), the ISP must restore access to same, unless the owner affected should submit the pertinent claim to the court, in which case it will be for the latter to decide. Liability is also attributed to any person who makes false complaints or notifications vis-à-vis material posted online.[231]

To my knowledge, there is still no relevant case-law in Morocco on the practical application of this Act. Furthermore, it should be noted that Morocco has been a signatory to the ACTA since October 2011, though this treaty had neither been ratified nor entered into force at the date of writing.

XII. COLOMBIA

At present, Colombia has no specific enactment that regulates the question of liability of internet service providers.[232] Consequently, the rules of the *jus commune* in civil and criminal matters are applicable.

This means that these cases are heard in criminal proceedings by reference to the rules of responsibility and co-responsibility laid down by the Penal Code (Articles 28 and 29) and the offences defined in Articles 270 (infringement of moral copyright) and 271 (copyright fraud).[233]

---

[230] Article 6.14 (A) of the Act.
[231] Article 61.14 (B) of the Act.
[232] At all events, in the implementation of Articles 20 (right to information) and 67 (right to education and access to knowledge) of the Colombian Constitution, Article 67 of the *2009 General Information & Communication Technology Act (1341*) provides that the State shall provide all Colombians with the right of access to basic information and communication technology, so as to permit the full exercise of the rights of freedom of expression and information, education, access to knowledge and science, etc. In addition, Act 679 of 3 August 2011 proposed, for the purpose of preventing child pornography, the creation of a code of conduct that would serve for ISP self-regulation, a code that was effectively adopted in 2004. Article 5 of the Act moreover contains a definition of what is to be understood by the terms, "access provider" and "hosting provider".
[233] When confronted by a case of defamation, Article 222 of the Colombian Penal Code may also be applicable in respect of any person who publishes or reproduces an insult or defamation attributed to another.

The law applicable in the civil sphere is Copyright Act 23 of 28 January 1982,[234] and specifically Article 238 thereof pertaining to actions for compensation, which, insofar as the rules of participation in infringements are concerned, must be combined with the general rules of non-contractual civil liability (Article 2.341 of the Colombian Civil Code).[235]

The debate surrounding the legislation that ought to apply to this issue in Colombia has been affected by the recent entry into force (15.5.2012) of the 2011 United States-Colombia Trade Promotion Agreement (hereinafter referred to as the CTPA),[236] Chapter 16 of which is devoted to intellectual property rights. Under Section 16.11 (Enforcement of Intellectual property rights) of the CTPA, there is a sub-head entitled, "*Limitations on Liability for Service Providers*", which requires both States to establish legal incentives for service providers to co-operate with copyright owners in deterring the unauthorised storage and transmission of copyrighted materials.

The Contracting Parties are likewise required to establish limitations in the legislation to preclude monetary relief with respect to the intermediation activities cited in the Agreement, which correspond to those of mere transmission or provision of access,[237] caching,[238] storage at the direction of a user of material residing on a system or network controlled or operated by or for the service provider,[239] and search engines[240]

The Agreement also envisages that the limitations shall apply only where the service provider does not initiate the chain of transmission of the material[241] and does not select the material or its recipients (save in the case of search engines, which obviously entail some form of selection of material by the search-engine operator). The exemption from liability is made subject to the standard conditions in these cases,[242] which draw their inspiration directly from the DMCA. Hence, in proxy caching, for instance, the provider is required to comply with rules governing the refreshing, reloading or other updating of the cached material where specified by the owner of the cached material, to respect the restrictions on access to content matter established by the owner of such content (e.g., passwords), and not to tamper with the systems for keeping a tally of visits to the web pages ("hits") established by the owner thereof, etc.

The limitation of liability for hosting service providers and Internet search-engine operators is subject to their not receiving a financial benefit directly attributable to the infringing activity and not having actual (effective) knowledge of the infringement, or, upon obtaining such knowledge, to their expeditiously removing or disabling access to the material residing on their system.
For the purposes of having actual knowledge of the illegality of the material, notification served by means of the notice and take down process that the Agreement itself requires the parties to adopt under Clause ix) of this Section, is deemed to suffice. To this end, the service provider must publicly designate a representative to receive such notifications.[243]

---

[234] The text of the Act is available at <http://www.wipo.int/wipolex/es/text.jsp?file_id=126025>.
[235] There are also laws governing liability for the acts of another in the case of persons to whom a duty of supervision and care is owed, such as parents with respect to children under the legal age of majority or employers for the conduct of their employees (Articles 2.247 to 2.249 of the Colombian Civil Code)
[236] The text of the Treaty is available at <http://www.tlc.gov.co/publicaciones.php?id=727>.
[237] Clause i), subsection A).
[238] Clause i), subsection B).
[239] Clause i), subsection C).
[240] Clause i), subsection D).
[241] Clause ii).
[242] Clause iv).
[243] Clause v), subsection C).

The Agreement also requires that the national legislature render recourse to safe harbours conditional on a policy being adopted and implemented which enables the service to repeat infringers to be terminated, and expressly establishes the absence of any obligation to monitor the possible existence of illegal content matter.[244]

In the case of mere conduit (transmission and access) activities, a possibility is left open for the national legislation to establish interim measures or actions for injunctions to remove material or prevent infringement, though in all cases limited to terminating specified accounts or taking reasonable steps to block access to a specific (non-domestic) online location.[245]

With respect to the other three intermediation activities envisaged under the Agreement (*hosting*, *caching* and search tools), the national Act must furnish the court with the means to order the removing or disabling of access to infringing materials, provided that, within all the measures which the court may adopt to prevent the infringement, such remedies of disablement or removal are the least burdensome to the service provider. On ordering the remedy of removal or disablement, the court must moreover have due regard for criteria such as the relative burden posed to the service provider in adopting the measure, the technical feasibility and effectiveness of the remedy, the harm to the copyright owner, and whether less burdensome, comparably effective enforcement methods are available to prevent the infringement.[246]

Lastly, the Treaty requires both Contracting Parties to penalise any person who wilfully makes a material misrepresentation in a notification or counter-notification, to exempt from liability for claims for compensation any ISP who removes content in accordance with the notice and take down process envisaged under the national legislation[247] and to establish in such legislation the obligation for providers to furnish any information they may have about alleged copyright infringers,[248] in a manner similar to that seen in the case of the DMCA *subpoena*.[249]

Following on from these Agreements, the Colombian Government has made a legislative attempt to regulate the issue of ISP liability by Bill No. 241 of 4 April 2011, governing liability for online infringements of copyright and related rights (a Bill popularly called the "Lleras Act" after the Minister of the Interior who tabled it before Congress).[250] The Preamble expressly mentioned the CTPA with the United States as being the fundamental reason for the regulation, which was in turn inspired by §512 of the US Digital Millennium Copyright Act.

The Bill defined the various roles of ISPs (Article 1) and established the general liability of Internet publishers in accordance with the general rules of civil, criminal and administrative liability (Article 2).

It also laid down the absence of any general monitoring obligation (Article 3) and a general principle of exoneration from liability (Article 4) if the requirements and conditions stipulated for each type of intermediary were met.

---

[244] Clause vii).
[245] Clause viii).
[246] Clause viii), *in fine*.
[247] Clauses ix) *in fine* and x).
[248] Clause xi).
[249] It appears that the Colombian Government was initially opposed to this procedure, which was nonetheless finally included in the FTA. This is asserted by RÍOS RUZ, R.W., *La Propiedad Intelectual en la era de las tecnologías de la information y comunicaciones (TIC's),* Universidad de los Andes, Bogotá, 2009, p. 607.
[250] Don Germán Vargas Llera.

With respect to the specific definition of safe harbours, the Bill strictly followed the FTA regulation outlined above, envisaging exemptions from liability for providers of data-transmission and internet-access services ("supply of connections", Article 5), providers of caching services carried out through an automatic process (proxy caching, Article 6), hosting service providers (Article 7), and Internet search engines (Article 8).

Article 9 contained a procedure for detecting and removing infringing content matter (applicable to all intermediation activities except those of mere conduit), modelled on the process envisaged under Section 512 (c) (3) of the DMCA, which was based on the principle of limitation of liability in any case where content was removed or access to it was disabled after receipt of notification under the terms of said Article (requirements which were set out in detail in Article 10). Such notification, complete with all the necessary detail, was to be delivered to the alleged infringer within a period not exceeding 72 hours.

The decision of whether or not to remove content depended, in principle, on the ISP, who was required to inform the supplier immediately of the removed content. Said supplier could then make a request to restore the material pursuant to the procedure laid down in Article 12 of the Act ("counter-notification procedure"),[251] a request that the intermediary then had to transfer to the notifying rightholder forthwith. If there was counter-notification, the intermediary had to restore the material online within a period of 10 to 14 days, save where the aggrieved rightholder filed a court action addressing the issue, in which case it was for the court to decide. In the absence of counter-notification, the ISP was required to remove the content, and was to be held harmless from any subsequent liability claims by the publisher.

As can be seen, in a case where there was no "counter-notification", content could be removed without judicial intervention, something to which public opinion reacted strongly. Finally, the Bill was rejected in November 2011, with the result that the text of the Act which implemented the CTPA into Colombian law in matters of intellectual property (Act 1.520 of 13 April 2012)[252] did not include rules governing ISP liability.[253]

As regards case-law on this issue, to my knowledge there are no court decisions in Colombia addressing ISP liability for copyright or related-right infringements.

XIII. RUSSIA

1. Legislation

Russian legislation contains no specific rules governing ISP liability. Internet service providers are exclusively subject to the provisions of the Communications Act and the regulatory provisions of the "rules for provision of telecommunications services", Rule 68 of which establishes a principle of exemption from liability for content sent or received by the recipients of their services.[254]

[251] This is the term used in the Preamble to the Bill.
[252] The text is available at website address <http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/ley152013042012.pdf>.
[253] Article 13 of the Act, however, establishes a prohibition on retransmitting television signals over the Internet without the permission of the rightholders, something that may have indirect repercussions for ISPs.
[254] NAUMOV, V. and AMOSOVA, A., "Provider's Liability", in AMCHAM News, Issue 88, available at <http://www.russianlaw.net/files/law/english/ae09.pdf>.

This law only applies, however, if the ISP has an administrative licence to operate (which, though usual in the case of access providers, is not quite as usual in the case of hosting service providers) and if it charges a monetary sum for the provision of the service (so that ISPs which provide charge-free hosting for blogs or social networks, for example, would not be subject to these regulations).

There is, moreover, an exemption from civil liability for enterprises that disseminate information on behalf of third parties (Article 17.3 of the Information, Information Technology and Protection of Information Act), if certain conditions are met (does not initiate the transmission; has no knowledge of the illegality of the information) but the Act itself (Article 1) expressly excludes infringements of intellectual property rights from its scope of application, so that it is only applicable with respect to other types of illegal conduct (e.g., attacks on good name, privacy, image, etc.).[255]

Furthermore, it should be borne in mind that at the date of writing (April 2012), a Bill to amend Article 1253 of the Civil Code had been passed on being given its first reading by the Russian Federal Parliament. With its new form of wording,[256] Article 1253.1 would establish a general principle of culpable liability for two specific types of ISPs (those which provide mere conduit and hosting services), with culpability being deemed to exist in any case where the requirements envisaged under Article 1253.2 (for mere conduit activities) or 1253.3 (for hosting service providers) were not met.

In the former case, the conditions required are: that the ISP in now way modify the information;[257] and that it neither know nor should have known that the activity undertaken by the recipient of the service was illegal.

In the latter case, in order for the hosting service provider to be able to benefit from the exemption from liability, it is essential that it neither know nor should have known that the content housed was illegal. As is usual in such cases, it will also be entitled to benefit from the safe harbour if, on receiving notification in writing from the owner of an intellectual property right, it acts expeditiously to take the *necessary measures* to eliminate the effects of the infringement. The specific scope of such "necessary measures" will nevertheless be determined in accordance with the provisions laid down in "legislation on information" (which I take to refer to a future reform of Article 17.3 of the Information, Information Technology and Protection of Information Act).

Until this bill has finally been approved, and in the absence of special laws *ratione materiae*, the general rules governing civil and criminal liability are applicable.

Accordingly, the provisions applicable are those of Part IV of the Russian Civil Code (RCC),[258] and Article 1255 and successive sections in particular, which specifically refer to copyright and related rights (Articles 1225 to 1254 contain a series of rules common to infringements of copyright and other immaterial rights, such as patents, trademarks and designs).

[255] See NAUMOV, V. and AMOSOVA, A., "Provider's Liability", in AMCHAM News, Issue 88, available at <http://www.russianlaw.net/files/law/english/ae09.pdf>.
[256] This is contended in the *2012 Special 301 Report* (12 February 2012) of the International Intellectual Property Alliance (IIPA), p. 101, available at website address <www.iipa.com>.
[257] The provision lays down that purely technical handling processes will not be construed as "modification" (e.g., the splitting of information into different packages to facilitate dispatch).
[258] Its text is available in English at website address <http://www.wipo.int/wipolex/es/details.jsp?id=11320>.

Despite being enacted more recently than the European and US regulations embodied in the DEC and DMCA respectively,[259] the Code does not however regulate the question of liability for aiding and abetting an infringement (secondary liability), an issue that has been the subject of intense debate in Russia and has led to the above-mentioned Proposal for Reform of Article 1253.

The Code nevertheless does contain an exclusive right to exploit a work for gain (Articles 18, 128, 1229.1, 1255.2 (1) and 1270), a right that includes communication on the Internet -Article 1270.2 (11) - as required by the 1996 WIPO Treaties (which entered into force in Russia in 2009). The RCC also establishes civil and criminal liability in cases of unauthorised use of intellectual creations (Article 1229.1 *in fine*).

Article 1.252.1 of the RCC contains a series of remedies which are common to all immaterial rights, including copyright and related rights, and which encompass actions for declaratory judgements, interim measures, actions for injunctions and an action for compensation for damage caused by any person who infringes exclusive rights.

For its part, Article 1250.3 clarifies the point that liability exists even in a situation where neither *mens rea* nor culpability is present in the infringer. Notwithstanding this, the Russian courts' interpretation is that the action for compensation continues to require culpability on the part of the infringer, thereby excluding the existence, in this respect, of a principle of objective or strict liability, something that might have considerably complicated the position of Russian ISPs in their intermediation work.[260]

By virtue of Article 1301 of the RCC, in lieu of compensation for damages, a copyright holder may opt for double the value of the copies, for the market value of the licence, or for statutory damages, to be set by the court at an amount ranging anywhere from a minimum of ten thousand to a maximum of five million roubles.[261] A similar rule is to be found in Article 1311 of the RCC with respect to related rights recognised by the Act.

Under Article 1252.3 paragraph two, in order to set the sum of such damages, the court must take into account the nature of the infringement and other circumstances of the case, having regard to criteria of reasonability and justice. Article 1252.3 paragraph three of the RCC affords the rightholder the possibility of claiming compensation for each act of infringement, individually or jointly, which is important in cases of mass rights infringement over the Internet.[262]

Since there are no special rules covering a situation where there are two or more infringers who collaborate jointly in the commission of the wrongful act, the general rules of non-contractual civil liability will be applicable to such cases, namely, Article 8.1 (6) of the Civil Code, which establishes the obligation to remedy the damage caused, and Article 1064.1 paragraph two of the RCC, which establishes that said obligation to make reparations may be imposed by law on a person other than that who caused the harm (e.g., parents with respect to damage caused by children aged under 14 years, Article 1073 of the Code)

---

[259] As from 1 January 2007, this Code replaced the earlier 1993 Copyright & Related Rights Act in order to better align the national law with the provisions of the Berne Convention and 1996 WIPO Treaties.
[260] This is the opinion expressed by NAUMOV, V. and AMOSOVA, A., "Provider's Liability", in AMCHAM News, Issue 88, available at <http://www.russianlaw.net/files/law/english/ae09.pdf>.
[261] The doctrine states, however, that it is not clear whether the "value of the copies" is that of the legal copies or that of those which are illegally marketed. See BUDYLIN, S., and OSIPOVA, Y., "IP Law Reform in Russia", *Columbia Journal of East European Law*, vol. 1, p. 14.
[262] If the infringer is a legal person, Article 1253 permits the court to order its liquidation in the event of serious or repeated infringements of exclusive rights.

In the absence of any such express legal provision, it would seem that, in principle, the rule to be applied is that he who directly causes damage must remedy it in full (Article 1064.1 paragraph one).[263]

It should nonetheless be borne in mind that Article 1081 of the Code expressly provides for shared liability in cases in which damage is caused jointly. This provision likewise makes it clear that it is for the judgement to allocate the share of liability which corresponds to each of those implicated. It would also appear that this provision may be applied to the case of Internet intermediaries, provided that the degree of causal connection between these and the damage caused directly by the end-users is deemed to be sufficient.

The Court may thus impose joint (joint and several) liability on all those responsible for the infringement, though Article 1081.2 of the RCC allows an action for contribution to be subsequently brought by the party who pays on behalf of the remaining debtors, claiming from each in proportion to his/her culpable contribution to the offence. Where compensation is not individually apportioned by the court, it will be allocated in equal parts. The internal relationship among the debtors is thus governed by rules of joint liability, though the existence *per se* of the action for contribution suggests that, when it comes to external relations (i.e., as between the holders of the intellectual property rights and the parties responsible for the infringement of said rights), the obligation is joint and several.

In the criminal sphere, the rule applicable is that contained in Article 146 of the Penal Code, which imposes prison sentences of up to six years plus a fine, for offences against copyright and related rights. In any case where there are two or more parties responsible for the criminal act, the rules applicable will be those governing co-responsibility and complicity under Articles 33, 34 and 35 of the Penal Code, and those of Article 33.5 in particular, which penalise any person who furnishes a third party with the means or instruments to commit the offence.

2. Case-law

The judicial situation of ISPs in Russia is far from clear and there is no discernable line in case-law[264] that would settle the question of liability of intermediaries, despite the fact that a good number of web pages are hosted on Russian servers, which serve as repositories of content for the exchange of files by end-users or as databases of hyperlinks for P2P applications.

a) *ISP liability*

[263] In addition, Article 1065.1 of the Code establishes an action for injunction to prevent harmful activities, which could be applied to the case of intermediaries if there is evidence of their causal contribution to the damage caused directly by the user. Such an action could also be targeted, according to Article 1065.2, at any enterprise or productive structure that continued causing or threatened to cause new damage.

[264] This has led to the fact that the cases which have had an impact in the news media have referred, not to intermediaries (indirect or secondary liability), but rather to direct infringers of intellectual property via web pages. This is the case of the well-known *AllofMP3* web page, which had two licences issued by the Russian rights management societies that were questioned by the Russian branches of the IFPI and RIAA, pleading infringement of Article 146 of the Penal Code, which is where the basic type of infringement of copyright and related rights is contained. The criminal courts dismissed the case against the owner of the website, which was nevertheless closed down shortly afterwards by an administrative decision of the Russian Government.

Apart from some precedent on the subject of the liability of hosting service providers for defamatory statements,[265] the leading case in this respect is that of *Kontent i Pravo v. Masterhost*, decided by the Supreme Court of Arbitration (SCA) on 23 December 2008.[266] In its award, the *Presidium* of the SCA for the first time decided a case of ISP liability for copyright infringement, and set the bases for establishing liability of hosting service providers, couched in terms similar to the form of wording used in the European Union's DEC.

In the case, the holder of the copyright in 18 musical files brought a claim against *Masterhost*, a company that provided physical hosting services on servers as well as technical support for the website from which these files had been made available. Instead of renting out server memory space, *Masterhost*'s hosting work thus consisted of placing the machines that contained the allegedly infringing websites inside refrigerated cages (an activity known as "housing").

The SCA held that the hosting service provider in this case was only performing technical functions, without even having access to the equipment from which the end-user posted the files online, so that in principle the party liable as principal infringer had to be said end-user. The Court went on to state that, in order to determine the intermediary's liability, it was important to take into account the fact of whether it knew or should have known of the existence of the copyright infringement that was being carried out by the subscriber to its services, knowledge which had to be proved by the party pleading infringement of its rights.

Based on these premises, the Court concluded that an ISP may only be liable if it initiates the transmission of the information, selects the receiver of the transmission or in some way modifies the information contained in the transmission.[267] Moreover, the end-user must be answerable for any content that he/she posts on the network. Furthermore, the fact that the agreement with the end-user contains rules allowing for the service to be suspended in the event that said end-user should use it to violate third-party copyright was held to be relevant for the purpose of establishing the degree of liability.

The Court took into account the fact that the ISP had collaborated directly in identifying the infringer, and that the copyright holder had failed to send any prior notice or notification to the intermediary before submitting the claim to the Court.

b) *Web 2.0 intermediation activities*

In the case of Web 2.0 intermediation activities, in 2011 the Supreme Court of Arbitration ruled that the social network, *VKontakte.ru*, could not be held liable for

[265] This is the case of *Troyka Stal' v. Megasoft,* March 2004, in which the Claimant sought to make a website operator liable for defamatory comments posted on the site by third parties. The lower court, in a second trial ordered by the Court of Cassation, found that the website administrator was to be deemed liable for the damage, due to having created the technological platform that rendered the defamation possible. See the reference to the case in NAUMOV, V. and AMOSOVA, A., "Provider's Liability", in AMCHAM News, Issue 88, available at <http://www.russianlaw.net/files/law/english/ae09.pdf>.

[266] No. 10960/2008. There is a translation and summary of the case in LABESUS, S., "Kontent i Pravo v. Masterhost, Presidium of the Supreme Arbitration Court of the Russian Federation, Judgement of 23 December 2008, No. 10962/08, Translation and Comment", *JIPETC*, 2010, vol. 1, pp. 179 ff.

[267] It should be borne in mind that the legislation applicable to the case was that contained in Articles 48 and 49 of the old Copyright Act, which established a principle of culpable liability, in contrast to the position under the current Article 1250.3 of the Russian Civil Code, which now establishes an obligation to remove infringing content in the event of continuous infringement. In this regard see LABESUS, S., "Kontent i Pravo v. Masterhost, Presidium of the Supreme Arbitration Court of the Russian Federation, Judgement of 23 December 2008, No. 10962/08, Translation and Comment", cit., p. 183.

copyright infringements committed by it end-users with respect to a file that contained a motion picture screened by the Russian state-owned broadcasting corporation, *RTL*.

The case arose from a decision of the Appeal Court, which, in July 2010, held that the social network operator had to pay one million roubles (approximately 25,200 euros) by way of compensation to the rightholders. Shortly afterwards, however, the judgement was overturned by a higher court, a decision that the SCA confirmed, taking into account the agreement reached by the parties whereby the network operator undertook to reveal the identity of the infringing user, who according to the Court, was the party that necessarily incurred liability in this case.[268]

Such agreements for deleting infringing content matter from this social network similarly exist with other rightholders,[269] though in practice each ISP decides individually whether or not it will collaborate with the rightholders.[270]

In another action involving social networks, the appeal decision of February 2012 of the St. Petersburg Court of Arbitration[271] held that *VKontakte.ru* had adopted an overly passive role in the infringement committed by one of its end-users (public communication of music files) because, instead of removing all the content from the end-user's account on obtaining notification from the aggrieved rightholder, it removed only those hyperlink*s* that appeared in the search results. It was therefore ordered to pay a sum of 210,000 roubles (approximately 5,300 euros) as compensation by way of damages.

c) *Internet search engines*

Insofar as Internet search engines are concerned, in June 2011 the Moscow Court of Arbitration issued a judgement, finding against the *Yandex* search engine and ordering it to pay compensation for the unlawful use of a dictionary of antonyms on the firm's portal. It seems, however, that the legal debate did not centre on the provision of hyperlinks by the search-engine operator to third parties but turned instead on the dictionary's reproduction on *Yandex*'s own servers.[272] Strictly speaking, therefore, this was not liability for aiding and abetting or "secondary" liability but rather a case of direct infringement.

In addition, a number of news stories have appeared in the mass media reporting that the search-engine operator *Google* has reached agreements with different rightholders, whereby websites which offered content that allegedly infringed property rights and others which contained hundreds of thousands of torrent hyperlinks would be blocked in its list of results*.*[273]

XIV. RWANDA

In Rwanda, protection for copyright and related rights is provided by Part III (Article 195 and successive sections) of the Intellectual Property Protection Act No. 31/2009 of

[268] A summary of the case can be seen at <http://www.ewdn.com/2011/03/16/russian-court-rules-social-network-not-responsible-for-user-copyright-violations/>.
[269] See the news summary at <http://www.petosevic.com/resources/news/russia>.
[270] As stated in the *2012 Special 301 Report* (12 February 2012) of the International Intellectual Property Alliance (IIPA), p. 95, available at website address <www.iipa.com>.
[271] A summary of the case can be seen at <http://www.ewdn.com/2012/02/22/vkontakte-ru-too-passive-with-copyright-infringement-says-arbitration-court/>.
[272] This, at least, is what is to be gleaned from the public summary of the case, available at <http://www.ewdn.com/2011/07/12/russia-tightens-screws-on-copyright-violations/>.
[273] As stated at <http://www.ewdn.com/2011/04/28/google-blacklists-pirate-sites-at-publishers-request/>.

26.10.2009, by establishing a series of moral (Article 199) and ownership rights (Article 200).[274]

Under Article 261, any infringement of copyright or related rights committed wilfully or with gross negligence by a third party is deemed to be a criminally punishable act of falsification, provided that said infringement is committed for gain. The Act extends criminal liability, not only to the principal offender (Article 261.2), but also to any third party who wilfully sells, offers for sale, rents, possesses or introduces into the territory of the Republic of Rwanda pirated goods for commercial or lucrative purposes (Article 264.4).

In the case of two or more offenders the general rules of co-responsibility and participation (Article 91 of the Penal Code) are applicable, a provision that contains a broad definition of the wrongdoer to include anyone who induces another to commit a crime or who knowingly harbours or conceals the offender.

In the civil sphere, the provisions of Articles 258 and 259 of the Civil Code are applicable.[275] These establish the general principle of non-contractual civil liability of a subjective nature, whereby anybody wilfully or culpably causing damage to another is required to remedy same.

In addition, a special regime of exemption from liability for ISPs is envisaged under Act 18/2010 of 12.5.2010, which covers electronic mail (e-mail), e-signatures and e-transactions[276] (Act 18/2010) and applies "horizontally" to all manner of illegal content (and not only to that which infringes copyright).

Article 8 establishes a total exemption from liability for online communications service providers in respect of content matter transmitted by their customers, provided that they have no control over such content. The definition of online communications services is to found at Article 1, No. 6 of the Act.

Article 10 of Act 18/2010 establishes a limitation of liability for any intermediary who provides *access* to, or *transmits or stores* information, provided that said intermediary complies with three general conditions common to all activities for which the Act affords a safe harbour (namely, it does not initiate the transmission, it does not select the receiver of the transmission, the functions are performed automatically, and it does not modify the information contained in the transmission).

Article 11 sets forth the specific conditions required to qualify for limitation of liability in proxy caching, specifying the standard conditions in this case (information not to be modified; updating of cached page to be permitted, etc.).

Article 12 lays down the conditions for exemption from liability of hosting service providers, stipulating that the provider must not have actual knowledge that the information harms third-party rights, nor be informed of facts or circumstances from which the illegal nature of the activity or the information stored is apparent (*constructive knowledge*). Furthermore, upon receiving notification pursuant to Article 14 of the Act, the provider must expeditiously remove or disable access to the online material.

---

[274] Furthermore, Article 204 of the Act contains a provision similar to that of Article 5.1 of Directive 2001/29/CE, governing temporary reproductions made in the process of transmission of works over the Internet.

[275] The Rwandan Civil Code was issued by Decree on 30 July 1888 and is available at website address <http://www.amategeko.net>.

[276] Official Gazette No. 20 of 17.05.2010. The Act is available at <http://www.wipo.int/wipolex/es/text.jsp?file_id=243157>.

The Act also envisages a limitation of liability for those providing tools for the location of information (Internet search engines), for which Article 14 requires that the provider neither have actual knowledge that the information harms third-party rights, nor be informed of facts or circumstances from which the illegal nature of the activity or the information stored is apparent. Furthermore, the provider must receive no benefit directly attributable to the infringing activity, and must remove or disable access to the infringing content matter within a reasonable time of receiving notification of the fact that said content infringes third-party rights.

The notification procedure outlined in Article 14 of the Act would seem to be of an exclusively private nature (without judicial or administrative intervention), given that service takes place directly between the aggrieved third party and the intermediaries. Such notification is to have a minimum content specified in this provision, with anyone sending notification to an ISP in bad faith (i.e., knowing it to be untrue) having to make redress for the damage so caused. There is also total exemption from liability for damage caused by the removal of materials as a result of false notifications.

To my knowledge, there have been no judgements rendered by the Rwandan courts in which Act 18/2010 has been applied to cases of infringement of copyright and related rights.

XV. SENEGAL

The Copyright and Related *Rights* Act No. 2008-09 of 25 January 2008 establishes the basis for protection of copyright in Senegal.

Protection is predicated on an exclusive ownership right to exploit the work for financial purposes (Article 33), a right that is protected by a series of special procedural mechanisms (Articles 127 and subsequent sections of the Act). Article 131 and subsequent sections lay down the procedures for interim relief, both specific under the Act (Articles 131-134) and general under the general civil legislation (Article 135). The Act also governs the criminal penalties for infringement of ownership rights (Article 143) and civil actions for injunction and compensation (Articles 151 and 152, respectively).

Save in the case of ISPs in the strict sense (which will be mentioned below), there are no specific rules governing secondary liability in the case of Internet intermediaries. In the field of criminal liability, the rules of the Penal Code[277] are thus applicable (Article 45 with respect to accomplices, Article 46 with respect to accessories before the fact, Articles 47 with respect to accessories after the fact, and Article 48 with respect to anybody who, knowing of the offence, fails to report it in the due manner). The statutory provisions applicable in the civil sphere are those of the New Code of Civil and Commercial Obligations,[278] which at Article 117 lays down the general principle of non-contractual civil liability, whereby anybody wilfully causing harm to another is required to make good the damage so caused.

For ISPs in the strict sense, the 2008-08 Electronic Transactions Act of 25 January 2008, establishes a spatial regime of liability for so-called "technical providers of services to the public using Internet technologies". These "technical service providers" are defined under Article 2 (3) of the Act as any operator that uses Internet protocols to place public or private, goods or services at the disposal of natural or legal persons.

[277] The Penal Code is available at <http://www.wipo.int/wipolex/es/text.jsp?file_id=181502>.
[278] The Code is available at <http://www.justice.gouv.sn/droitp/COCC.PDF>. The part of interest, relating to obligations, was approved by Act 63-62 of 10 July 1963.

In principle, therefore, the broad definition furnished by the Act includes, not only "classic" ISPs, but also suppliers of content, though in reality when it comes regulating the exemptions from liability, the Act refers exclusively to access and hosting providers (and not to providers of proxy caching or Internet search engines).

With respect to access providers, Article 3.1 of the Act confines itself to stating that, in their user agreements, these are required to make mention of the existence of means that would enable access to be restricted, without including specific conditions to govern a safe harbour for the purpose of eluding any possible liability for content transmitted.

In the case of the safe harbour for hosting service providers, Article 3.2 of the Act establishes an exemption from civil liability for content stored at the request of a recipient of the services,[279] unless the ISP has actual knowledge of its illegal nature or is unable to ignore facts or circumstances that render said nature apparent (constructive knowledge). The exemption from liability is similarly applicable in any case where an ISP, on obtaining knowledge of the illegality of the material housed, acts swiftly to remove the data or disable access to same. The provision is solely applicable to content matter that infringes copyright or related rights.

Article 3.3 of Act 2008-08 addresses the criminal liability of hosting service providers, by creating an exemption, if there is no actual knowledge of the illegality of the activity or if the content matter is removed or access to it is disabled as soon as said knowledge is acquired. This exemption will not apply in any case where the recipient of the service acts under the control or authority of the service provider.

Article 3.4 establishes a notification system whereby hosting service providers can be presumed to have actual knowledge in any case where said notification has the minimum content stipulated by the provision (date; identification of the holder; the allegedly infringing materials; etc.).

Lastly, Article 3.5 lays down the absence of a general obligation to monitor illegal content transmitted or housed, or to investigate facts or circumstances that reveal such illegality, without prejudice to any monitoring activity that may be ordered by a court on a temporary basis for a given case. Similarly, the courts are empowered -with respect to hosting service and access providers alike (Article 5.6)- to make an order in the form of interim measures or injunction to prevent or halt damage.

Furthermore, access and hosting providers are under an obligation to preserve the data of any person who has used their services to post content matter online, data that may be required by the court in the course of an investigation into an infringement, with due heed being paid to statutory protection of data of a personal nature (Article 4). ISPs must also display an announcement or sign which is clearly visible to the end-users of their services, stating that piracy is harmful to artistic creation (Article 7).[280]

To ensure that these obligations are met, Act 2008-11 of 25 January has introduced criminal penalties into the Penal Code for intermediaries who fail to comply with the

[279] This exemption from liability does not come into play in any case where the recipient of the service acts under the authority or control of the hosting provider.

[280] The website of the Senegalese Government announces the promulgation of the Decree governing electronic commerce, which implements the 2008-08 Electronic Transactions Act. Nevertheless, the text shown is still that of the Draft Decree (<http://www.adie.sn/IMG/pdf/Decret_relatif_au_commerce_electronique.pdf>).

provisions of Act 2008-8 (new Articles 431-44, 441-45 and 441-46 of the Penal Code).[281]

To my knowledge, there is no relevant case-law in Senegal on the application of Act 2008-08 to access or storage providers for infringements of copyright or related rights.

XVI. SPAIN

1. Legislation

a) *The legal regime of the Information Society Services & Electronic Commerce Act 34/2002*

The DEC was implemented in Spain by the Information Society Services & Electronic Commerce Act 34/2002 of 11 July[282] (hereinafter referred to as the ISSECA) (*Ley de servicios de la sociedad de la información*), which governs the issue of ISP liability in Articles 13 to 17.

Article 14 of the ISSECA establishes the limitation of liability for network operators and enterprises which provide Internet access services (mere transmission or mere conduit activities), regulating the matter in a style and manner almost identical to that of Article 12 of the DEC.

The safe harbour for proxy caching providers is governed by Article 15 of the ISSECA, which exempts intermediaries from liability with respect to the creation of temporary, provisional, automatic reproductions for the sole purpose of enhancing the effectiveness of subsequent data transmission to other recipients of the service who request these, provided that said intermediaries comply with the five requirements stipulated in subsections a) to e) of Article 15 of the ISSECA, which reiterate, almost point for point, the provisions of the Directive on Electronic Commerce.

The liability of hosting service providers is regulated by Article 16 of the ISSECA, which implements Article 14 of the DEC in Spanish law. The ISSECA exempts these providers from liability where they have no actual knowledge that the information stored is illegal or that it harms third-party goods or rights in respect of which compensation is payable. They are likewise exempt in any case where they obtain such actual knowledge but act diligently to remove or disable access to the data.

The Spanish legislature has, however, disregarded the reference made by the DEC to the fact that, for the purpose of actions for compensation, hosting service providers may not ignore facts or circumstances that render the illegal nature of the activity or information apparent, thereby omitting the concept of constructive knowledge under Article 14 of the DEC.

Furthermore, the Spanish legislature has put forward a definition of actual knowledge (Article 16.1.II of the ISSECA), laying down that such knowledge only exists in a case: where a competent body has declared the illegality of the data and the provider is aware of the judgement; where the provider has failed to apply a voluntarily adopted

[281] This Act also states that, in the event of a criminal offence via the Internet service, the court may order a temporary or definitive halt to be brought to the means used to commit the infringement (new Article 431-64 of the Penal Code).

[282] Official Government Gazette of 12 July 2002, No. 166. The Act as a whole came into force on 12 October 2002 (Final Provision 9).

detection and removal procedure; or where, by *any other means that might be put in place*, the provider acquires such knowledge.[283]

Article 17 of the ISSECA, by way of a novelty vis-à-vis the DEC, has tackled the issue of liability for the establishment of hyperlinks to web sites supplying illegal content or that of Internet search engines, by providing a safe harbour if the conditions stipulated in said Article are met.

In order for the exemption to apply, the operator of the linked page must not be under the control or responsibility of the person who has created the hyperlink,[284] the provider of the hyperlink or search engine must have no actual knowledge[285] that the activity or information to which browsers are directed is illegal, or, in any case where it does have such actual knowledge, it must act diligently to remove or disable the pertinent hyperlinks (Article 17.1 (b) of the ISSECA). These are, in essence, the same requirements demanded of hosting service providers, though in this case the illegality logically refers to the linked content and not to that housed on the operators' own servers.

Lastly, mention should be made of the fact that the ISSECA has not expressly implemented Article 15.1 of the DEC, and establishes an obligation of collaboration with the authorities in specific cases only (Articles 11 and 12 of the ISSECA). Accordingly, recourse must be had both to interpretation under the national law consistent with community law, and to CJEU case-law, in order to justify the absence of a general monitoring obligation in Spain.

b) *Additional Provision 43 of the Sustainable Economy Act*

The Spanish legislature has sought to find a solution to the problem of link-listing websites (not settled in Spanish case-law, as will be seen below) through the introduction of a reform in Additional Provision 43 of the Sustainable Economy Act 2/2011 of 4 March. This provision adds a new Section 2 to Article 8 of the ISSECA, with the aim of enabling accurate identification of "those responsible for the information society service" who engage in conduct that allegedly infringes copyright[286]

Coupled with this identification mechanism (which partly solves the problems that arose in Spain as a result of the CJEU's decision in the *Promusicae* case)[287] is a new hybrid

[283] M. Peguera states that, thanks to this definition, and in the absence of a notice and take down procedure in the DEC or Spanish legislation, the Act confers almost total immunity on Spanish hosting service providers, though Supreme Court case-law has qualified said immunity by allowing alternative ways of showing effective knowledge of the illegality of content. See PEGUERA, M., "Internet Service Providers' Liability in Spain", *JIPITEC*, 2010, No. 1, p. 153.

[284] This is to be understood from Article 17.2 which, in the wording of Act 56/2007 provides that, "*the exemption from liability stipulated under Section 1 shall not operate in any case where the supplier of the content to which the link leads (...) acts under the direction, authority or control of the provider that facilitates the location of such content*".

[285] To define what amounts to “effective knowledge” of the legality or illegality of linked content, Article 17.1 paragraph two reproduces, point for point, the concept of “effective knowledge” established for hosting service providers under Article 16.1 paragraph two.

[286] In order to be able to carry out such identification, the *competent bodies* (which include an administrative body created *ad hoc* for the purpose, Section Two of the Intellectual Property Board) may require the information society service provider to produce the personal data of the (alleged) infringer so that the latter may appear in the procedure for suspension of the service in question (e.g., the removal or blocking of content on web pages). To require production of such data a prior court order is needed, in accordance with the terms of Section one of the new Article 122 b of the Act regulating contentious-administrative jurisdiction (a provision also introduced by this Additional Provision 43 of the Sustainable Economy Act).

[287] Decision of the Court of Justice of 29 January 2008, case C275/06, which held that EU legislation did not require Member States to establish in their national legislations this duty of delivering up the data of copyright infringing users in the framework of civil proceedings.

administrative and judicial procedure, which empowers an *ad hoc* administrative body (Section Two of the Intellectual Property Board) to determine whether the content supplied to a web page violates third-party intellectual property rights and to order ISPs to remove or disable access to it (Article 158.4 of the Intellectual Property Act).[288]

2. Case-law

a) *Web 2.0 intermediation activities*

The Spanish Supreme Court (SC) has issued a comprehensive interpretation of what is to be understood by "actual knowledge" under Article 16.1 of the ISSECA, holding in its decisions of 9.12.2009[289] ("*putasgae*" case), 18.5.2010[290] ("*quejasonline*" case) and 10.2.2011 ("*A las barricadas*" case),[291] in different cases of attacks on the right to a good name, that the existence of actual knowledge may also be shown on the basis of the communication made by the aggrieved person or on the basis of other data that enable this to be proved *ex re ipsa* [i.e., *res ipsa loquitur*] (as occurs, for instance, where a direct insult is proffered). The Supreme Court thus construes the provision in accordance with the DEC, deeming that there may *also* be actual knowledge in a case where there is evidence of facts or circumstances from which the activity or information is apparent (constructive knowledge).[292]

This doctrine has been applied in the case of operators of websites, blogs or fora that permit comments from end-users, activities which, according to Spanish case-law, all come within the safe harbour described in Article 16 of the ISSECA.

This is a doctrine which may also be applied by analogy to other cases of Web 2.0 electronic platform operators, as was done for instance by the decision of Madrid Commercial Court No. 7 of 20.9.2010 (*Telecinco v. YouTube*)[293] in a case akin to the well-known case of *Viacom. v. YouTube*. The Court stated that the activity of the video-exchange platform operator could be brought within "intermediation" in the sense of the Spanish ISSECA, implying in turn that the "non-monitoring rule" of Article 15 of the Directive would be applicable to it.[294]

---

[288] Section Two will be able to adopt such measures on condition that the provider acts for gain, direct or indirect, or has caused or *may cause* pecuniary loss. Nevertheless, the Board itself may not enforce the measure: to this end, it must seek the aid of a court having contentious-administrative jurisdiction, which must accept the proposed measure or, alternatively, reject it if it deems that said measure restricts the freedom of expression protected by Article 20 of the Spanish Constitution (Article 122 b of the Contentious-Administrative Jurisdiction Act).

[289] Court 1, RJ 2010/131, *SGAE v. Asociación de Internautas.* The Supreme Court held that the website operator had effective knowledge of the illegality of the injurious comments made, with the result that it was unable to benefit from the exemption of Article 16.1 b) of the Spanish ISSECA.

[290] Court 1, RJ 2010/2319, *Luis Alberto v. Ruboskizo S.L.* In this case, a Valencian attorney claimed against a website devoted to enabling users to express their complaints, since one of these users, usurping the attorney's identity, had insulted one of his clients. Following the attorney's complaint, the web page operator removed the comment immediately but refused to furnish the identity of the person responsible. The Supreme Court held that exemption from Article 16 of the ISSECA applied here because the hosting provider's rapid reaction warranted this.

[291] Court 1, *José Ramón Márquez Martínez (Ramoncín) v. Xorxe Oural Martínez*. The decision is available at <http://s.libertaddigital.com/doc/sentencia-del-supremo-que-condena-a-la-web-alasbarricadas-a-indemnizar-a-ramoncin-41912140.pdf>.

[292] Its doctrine may however also be applied by analogy to the case of violations of copyright, in view of the fact that the regulation imposed by the ISSECA (like that of the Directive on Electronic Commerce) is of a horizontal nature.

[293] Madrid Commercial Court No. 7. There is an English translation of the decision available at <http://www.jipitec.eu/issues/jipitec-1-3-2010/2797/Telecino.pdf>.

[294] The court also held that, in order to enable *YouTube* to have effective knowledge of the illegality, the owners would have to identify individually the specific files that infringed their rights. The pertinence of the action for injunction was rejected on the ground that there was an exemption from liability, in contrast to the provisions laid down in Articles 138. III and 139.1 h) of the Spanish Copyright Act.

b) *Internet search engines*

In the case of Internet search engines, the Barcelona Provincial High Court's (Section 15) decision of 17.9.2008[295] held, in a case of temporary reproductions made by the robot of the search-engine operator, *Google*, that such activity was not covered by the exemption from liability under Article 17 of the ISSECA (which refers to the provision of hyperlinks, and not to copies made by search-engine robots on their own servers). The Barcelona Provincial High Court held further that neither could a "safe harbour", as envisaged under Article 15 of the ISSECA for proxy caching, be deemed to exist in cases such as these, since one was dealing here, not with an ISP that was *transmitting* information, but rather with a search-engine operator that *was storing* it.[296]

The Madrid Provincial High Court's decision of 19.2.2010[297] (the "*Aquí hay tomate*" case) applied the exemption from liability under Article 17 of the ISSECA to a case in which an individual sought compensation by way of damages from the search-engine operator, *Google*, for displaying hyperlinks to a web page containing harmful statements that were prejudicial to the Claimant's good name. The Court deemed that the search-engine operator had no actual knowledge of the defamatory content, by reason of the fact that it did not have a copy of the court decision declaring this to be so (the Claimant had furnished information about the court's ruling against the web page, without providing the text).

c) *Hyperlinks to download sites containing illegal content matter*

There are many court decisions in Spain which have ruled on the question of the liability of those who provide hyperlinks that direct end-users to web pages which function as digital file storage facilities, or which enable P2P customers to exchange files or TV programs via online streaming, by supplying hyperlinks that the end-users can activate to initiate the exchange.[298]

In the criminal sphere, the line followed by most of the judgements issued by the Spanish Provincial High Courts is that the offer of hyperlinks to third parties over web pages specifically dedicated to this goal does not amount to an infringement of rights, if the content matter is not housed directly (it being deemed that there is neither reproduction nor public communication of the linked content matter). As a consequence, there can be no room for actions claiming criminal liability pursuant to Article 270 of the Spanish Penal Code, which contains the basic types of offences against intellectual property.[299]

---

[295] *Megakini v. Google,* AC 2008/1773.

[296] Even so, the Court also held that the copies stored by Google on its servers deriving from searches conducted by its engine, amounted to a *usus innocui* of the protected works and could, moreover, come within the supposed limit envisaged under Article 40 b of the Spanish Copyright Act, so that no evidence of an infringement was to be found. It stated further (along the lines followed by the German Supreme Court) that there was a sort of implicit consent to these types of reproductions on the part all persons who posted material online.

[297] JUR 2010/13310.

[298] In view of the great number of these, I have decided to omit judicial rulings (orders or decisions) issued by the Courts of First Instance and exclusively highlight the basic lines laid down by the Supreme Court or Provincial High Courts (courts of second instance or appeal).

[299] For this reason, the dismissal of the case ordered by the Examining Magistrate's Court is normally upheld. A comprehensive list of same is available at website address <http://responsabilidadinternet.wordpress.com/resol_jud/webs_enlace/>, with the first of these being the court order of the Barcelona Provincial High Court of 22.12.05 (confirming the acquittal of the Defendants) and the last, to date, being the court order of the Álava Provincial High Court of 3 February 2012 (confirming the dismissal of the case).

Accordingly, the Spanish Courts have focused on the absence of an act of direct exploitation by the web-page owner and on the fact that, in Spanish law, end-users who do not act for gain, commit no offence whatsoever, thus rendering it impossible to speak in such a case of complicity with this conduct. Moreover, the courts have often added by way of *obiter dicta* that such conduct is covered by the exemption afforded by Article 17 of the ISSECA.[300]

Even so, there is also a second minority line of court decisions.[301] These hold that the operators of these hyperlink pages should be found guilty of an offence against intellectual property under Article 270 of the Penal Code, deeming, in general, that supplying hyperlinks to third parties implies the undertaking of an act of communication of content to the public in the capacity of the direct or principal offender, without web-page owners being entitled to benefit from the exclusion of liability under Article 17 of the ISSECA due to their being aware of the illegality of the linked content.

In the area of civil liability for hyperlink pages, attention should be drawn to the judgement handed down by the Barcelona Provincial High Court on 24.2.2011 (case of *elrincondejesus.com*),[302] in which, in an openly contradictory manner, liability was held not to exist in the case of the hosting of hyperlinks that initiated downloads via P2P applications but was nevertheless held to exist with respect to hyperlinks to digital storage facilities (known in the jargon as "direct download links").[303] Subsequently, however, the decision of the same Barcelona Provincial High Court of 7.7.2011 (*Indiceweb* case),[304] rectifying the error committed in the above-mentioned decision, now ruled that, in its view, there was also no act of communication to the public by reason of supplying "direct download links". In addition, the Barcelona Provincial High Court stated that Article 17 of the ISSECA was not applicable in this case.

d) *Distributors of file-exchange programmes.*

In the case of distributors of P2P file-exchange programmes, the decision of Madrid Commercial Court No. 4 of 25.11.2011[305] dismissed the action and corresponding claim for compensation by way of damages brought against the parties responsible for various programmes, holding that the provision applicable to the case ought to be Article 1903 of the Spanish Civil Code (vicarious liability), and that the requirement of a relationship of dependency or control between the distributors of the software and the recipients who used it had not been met.

---

[300] The leading case on the subject is the "Sharemula case", Madrid Provincial (Criminal) High Court order of 11 September 2008, as PEGUERA, M. correctly points out in, "Internet Service Providers' Liability in Spain", *JIPITEC*, 2010., No. 1, p. 162.

[301] Some of these order the criminal proceedings to be continued (this is the case of the Vizcaya Provincial High Court order of 27.09.2010, Palma Provincial High Court order of 20.10.201, Alicante Provincial High Court order of 20.9.10, and Madrid Provincial High Court order of 28.6.10, etc.). There are also at least three decisions handed down by courts of first instance, in which there is a sentence resulting from a plea bargain (acknowledgement of the facts by the Defendant), and a sentence of the Vizcaya Provincial High Court of 27.09.11 (*caso fenixp2p and mp3-es*). The text of these decisions is available at <http://responsabilidadinternet.wordpress.com/resol_jud/webs_enlace/>.

[302] The text of same is available at website address <http://estaticos.elmundo.es/documentos/2011/03/sentencia_rincon.pdf>.

[303] In the first case, the Barcelona Provincial High Court held that there had not been any act of public communication, whilst in the second it held that there had (doubtless deeming, in error, that the content had been supplied from the Defendant's web page, when in reality it had been housed on external servers). This same confusion can explain why the Provincial High Court did not go into the matter of the possible application of Article 17 of the ISSECA, with respect to the exemption from liability for furnishing links, a provision that is intended for cases of intermediation rather than for direct supply of content to third parties.

[304] Available at <http://www.filmica.com/david_bravo/archivos/sentencia.pdf>.

[305] The decision is available at website address <http://www.abc.es/gestordocumental/uploads/Cultura/sentencia_pablo_soto.pdf>.

XVII. CONCLUSIONS

1. Liability of ISPs in the strict sense (access and hosting providers)

a) *Civil and criminal liability*

With respect to the liability of Internet service providers, there is a clear division in the 15 legal systems reviewed between countries which possess special legislation to exempt ISPs from liability and those in which the general rules of the *jus commune* in civil and criminal matters are applied.

i. Countries with specific legislation governing ISP liability

Within this first group, there is, in turn, a sharp contrast between European Union countries where the rules of the Directive on Electronic Commerce -as interpreted by the CJEU- are applied, and countries where regulation is based on the USA's DMCA, which, through the Free Trade Agreements, has inspired the regulation now in place in some Latin American countries (Chile and Colombia, though in the latter case the issue was left pending in the most recent law reform, for political reasons) and in African countries, such as Morocco.

Hence, whereas the former use a "horizontal" approach to regulate ISP liability, the latter address the issue from the specific stance of infringements of copyright

At all events, in both groups of countries, the problems of liability relating to transmission or caching activities aimed at accelerating online data-transmission can be seen to be practically non-existent.

Also evident is the fact that, insofar as network access providers are concerned, the problems which have arisen in the jurisdictions studied have not been connected so much with their civil or criminal liability (in the great majority of cases, the conditions of neutrality required by statute or case-law are substantiated) as with their role when it comes to blocking end-user access to the network (actions of temporary disconnection in "graduated response" systems, or actions to prevent end-users with active connections from gaining access to pages or sites that are used to infringe copyright, basically pages supplying hyperlinks).

The most relevant problems concerning liability have basically been posed in respect of hosting service providers and, in many instances, have been due to the absence of a notice and take down process which would manifestly afford proof of the ISP's actual knowledge of the illegality of content (a procedure that does, however, exist in enactments modelled on the DMCA, such as those of Chile, Colombia, Morocco and Rwanda).

Indeed, in the absence of a harmonised notice and take down process, the real bone of contention in the case-law of European Union countries is the question of the means whereby an ISP can be deemed to be shown to have actual knowledge of the illegality of material. Indeed, this has led to one Member State (Finland) having decided to lay down its own procedures in its national law to establish, in the most effective manner, the precise point at which a hosting provider can be deemed to become aware of the illegality of the material housed, thus marking the commencement of the time limit for it to take expeditious action to remove or disable access to such content.

In practice, important differences are to be seen among the jurisdictions reviewed as to whether the existence of a duly notified judicial or administrative judgement is required or, on the contrary, whether notification by the parties involved would suffice.

There is, however, agreement in the enactments of the countries studied as to the fact that, in order for criminal liability to be attributable, there must be actual knowledge of the unlawfulness of the content, which implies finding *mens rea* on the part of the ISP as regards the conduct of the end-user of its services, whereas in order for civil liability to be held to exist (embodied in an infringement giving rise to damages), the standard required is much lower, with it sufficing for the ISP to know the facts or circumstances that make the illegality of the content apparent (constructive knowledge or reckless disregard/*dolus eventualis*).

There is no agreement, however, as to when such reckless disregard exists. The statutes tend to mention the fact that the content matter must be clearly unlawful, obviously unlawful or manifestly unlawful, yet there is considerable variation in the criteria followed in the case-law of the respective States.

Similarly, there is no agreement on whether it is possible for a hosting provider to benefit from the exemption even in a case where it obtains a financial reward. The DEC makes no mention of the profit motive as a criterion that would act as a bar to benefiting from the limitation of liability. Nevertheless, in some of the countries studied (such as Chile), the national law requires that, in order to be eligible to benefit from the limitation of liability, no financial reward directly attributable to the illegal activity may be obtained. The same occurs in Colombia, where the FTA with the United States requires that the safe harbour be conditional upon receiving no financial benefit directly attributable to the infringing activity.

ii. Countries without specific legislation governing ISP liability

Where there is no special legislation governing ISP liability, the countries studied have encountered considerable difficulties in having recourse to the doctrine of complicity, aiding and abetting or co-responsibility (with the pertinent national terminology in each case), in order to attribute criminal liability to anyone who, without being a direct infringer of exclusive rights, nonetheless co-operates with such offenders (Internet end-users) in the infringement of copyright.

Although this possibility is generally accepted by the doctrine in each of the different jurisdictions, the truth is that, in practice, there are hardly any judgements that venture to take the step of attributing criminal liability for copyright infringements to ISPs (in reality, to the natural persons who are in charge in each case), in the absence of a statutory provision that specifically regulates the matter. The few criminal sentences that do exist in this regard (e.g., in the Taringa! case in Argentina) tend to refer to digital storage facilities in which illegal content matter is filed or to hyperlinks to torrent download sites.

The situation is equally hazy in the field of civil liability because, in this instance, there is the essential difficulty that in many of the countries with a civil law tradition the concept of liability by contribution (secondary liability) is not developed along the same lines or with the same scope as in countries with a common law tradition.

This is due to the fact that, though it is generally accepted in the majority of the countries studied that civil liability must be attributed to anyone who induces or contributes to the infringement of copyright committed by another person, this is achieved by the indirect mechanism of establishing indiscriminate (joint and several) liability as between the principal offender and the accessory. Furthermore, in line with the general rules of non-contractual civil liability in force in continental law, each case must be examined on its merits to ascertain whether there is sufficient causal connection with the criminal act to rule that there has been an infringement, something

that has generated contradictory judgements in case-law in situations where the facts of the case were almost identical.

In these countries without special legislation on ISPs, it is not, however, possible to apply the rules of the *jus commune* regarding liability for the act of another (vicarious liability), since most of the cases analysed fail to meet the requirement that the direct offender act under the control or supervision of the intermediary sought to made liable. It is also generally rejected that the system to be applied to intermediaries (and to hosting providers in particular) is objective liability in accordance with risk theory.

It should be noted that in practically all the countries in which the adoption of specific legislation on this issue has been or is being discussed (e.g., Mexico, Argentina, Brazil, Colombia and Russia) there is a substantial degree of public reaction and debate on the matter, something that, in turn, places important political obstacles in the way of achieving a consensus solution that would make the adoption of legislation possible. These same difficulties also arise where a solution is proposed in a multilateral treaty, such as the ACTA or Trans-Pacific Partnership Agreement.

b) *Specific duties linked to interim measures and actions for injunctions*

In general, the jurisdictions studied display notable differences when it comes to interim actions and injunction measures, which suggests that this is an aspect that presents difficulties for achieving common solutions at international levels.

Moreover, the existence of a general duty to monitor content matter is rejected in practically all the jurisdictions studied, with respect not only to transmission and network access (mere conduit) activities, but also to the hosting of information. In some countries, however, the question has been raised as to whether ISPs have a duty to prevent or mitigate future infringements.

Indeed, in some European jurisdictions -as a reflection of the DEC's failure to harmonise this issue- there are a great number of judgements, in countries such as France, Germany and Italy, which hold that in respect of content *already declared unlawful* by a judicial or administrative ruling of a competent body, or in respect of which the ISP *clearly* knows its illegality (e.g., because it has been notified thereof by the rightholders), there is a duty on the part of intermediaries (particularly, in the case of hosting service providers) to prevent new infringements.

This must be achieved by using measures that are proportionate, effective, dissuasive and do not impose disproportionate obstacles on e-commerce, though it is not clear to what extreme an intermediary must go for it to be deemed to have made a reasonable effort, in accordance with the state of the art of the technique at hand, to prevent such future infringements.

There is also a still unresolved debate in the European Union regarding the obligation of hosting service providers and Web 2.0 electronic platforms with respect to prior filtering of content matter (the CJEU's decisions in the *Sabam* and *Netlog* cases).

2. Liability of Web 2.0. electronic platform intermediaries. Application of the exemption of "hosting" to these cases.

This study has shown that the regulations in force in most of the countries fail to take the Web 2.0 phenomenon into account, where it is the end-users themselves who, with the aid of the electronic platform operated by a third party, exchange content matter that may affect copyright.

Most countries would agree that the legislation governing ISPs is out of date in this regard, on drawing a rigid distinction between hosting service providers and publishers. It is usually said in these cases that the platform operator's task is not confined to performing a mere activity of intermediation (such as that performed by hosting service providers, who restrict themselves to earmarking space on their servers for a third party to house content), and yet neither does it have such an intense level of prior control of content that would allow it to be equated with a publisher.

Hence, the difficulties experienced by the courts in the respective countries to find a uniform solution to such situations will come as no surprise. In the sphere of European Union in particular, CJEU case-law in *Lancome v. Ebay* could serve as the starting point for the adoption of different solutions in each of the Member States, in accordance with the factual circumstances of the case.

In very general terms, there seems to have been a discernable trend in EU case-law to date to consider it possible for Web 2.0 electronic platform operators (social networks, web pages for the exchange of files or goods) to benefit from the exemptions envisaged under Article 14 of the DEC, though conducting a case-by-case analysis in every instance to see if the requirements of neutrality or passivity stipulated by Community law are met.

In France, for example, different Appeal Court judgements have stated that the presence of a profit motive in a specific service (that of sponsored hyperlinks) would not bar a search-engine operator from benefiting from the exception under Article 14 of the DEC, if the search-engine operator were unaware of the illegal nature of the information furnished by the advertiser.

In another Web 2.0-related case, however, the French Court of Cassation held that *Ebay* did not perform a simple hosting activity totally independent of the activity of the vendors of counterfeit products. Instead, it played an active role which gave rise to knowledge or control of the data that it was storing, and so deprived it of the exoneration from liability enjoyed by hosting providers.

In other legal systems in which there is no specific legislation in this regard, thanks to the growing body of case-law the idea is gradually becoming accepted that Web 2.0 platform operators should enjoy a limitation of liability with respect to content exchanged by end-users, and that this limitation is only lost where they know of the illegality of such content or where they fail to remove it from the system after receiving duly certified notification from the intellectual property rightholders. Hence, a number of decisions of the Argentine Courts and the Brazilian High Court of Justice have, for instance, held that in cases of infringement of personality rights (basically through social networks), Web 2.0 platform operators are not subject to liability, provided that they take immediate or vigorous action to remove the infringing content matter. There is likewise the conviction in these countries that this doctrine can be extended by analogy to infringement of copyright, though as yet there have been no final decisions on the issue in the majority of cases.

At all events, it is plain from the study of the countries analysed that, little by little, the idea is taking shape that the standard of professional diligence owed by these Web 2.0 operators is, on the one hand, higher than that of a mere passive intermediary, thus requiring them not to ignore facts or circumstances which clearly reveal the unlawful source of the content matter being exchanged by end-users over their systems, and, on the other hand, lower than that of a publisher, who has full control over content.

This implies deeming that wilful blindness by Web 2.0 intermediaries vis-à-vis acts which are clearly prejudicial to third-party interests is not acceptable, and that both an investigation conducted by the intermediary itself and a duly certified notification accepted by it are to be admitted as valid means of obtaining knowledge or awareness of illegality, provided that said notification fulfil the minimal requisites of formality, accurate and complete identification of the rights affected, etc.

3. Pages containing hyperlinks to content that infringes copyright

In the case of web pages which contain lists of hyperlinks to illegal content matter housed in the digital repositories of third parties or to files that are exchanged over P2P networks, this review shows that there is no legislation in this regard in any of the legal systems analysed, and that the response given by the courts differs according to the facts of the case and the perceived degree of linkage with the illegal content to which these connect (actual knowledge of and causal contribution to the offence).

Generally, account is also taken of whether there is any direct or indirect financial gain involved in the activity of providing hyperlinks. On this basis, the courts in the respective countries (with an occasional exception, such as Spain) tend to conclude that what these websites are endeavouring to do is to attract end-users so as to obtain a direct or indirect financial reward, the ground upon which they are thus to be held civilly and/or criminally liable for the infringement of intellectual property rights (in this regard, there are cases before the Supreme Courts of Finland and Germany).

Furthermore, in many jurisdictions there are court decisions that require ISPs to block end-user access to these types of pages (this is what occurs, for instance, in Belgium, Finland and Italy).

4. Internet search engines

Among the jurisdictions studied, there is wide diversity regarding the liability regime that should apply to Internet search engines. What decisively contributed to this state of affairs was the fact that the EU Directive on Electronic Commerce left this question out of the harmonisation, something that has led to differing responses in both the case-law and legislation of European countries.

Specific regulation of this issue is also to found in some countries outside the European sphere, owing to the influence of the DMCA (i.e., the case of Chile, Rwanda and Morocco), where, in the concrete case of search engines, the view tends to be held that the requirement (demanded of the remaining ISPs) that they select neither the content matter nor the recipients thereof, is not applicable, since such selection forms an intrinsic part of the functioning of Internet search-engine operators.

In those legal systems in which there is no specific legislation addressing this question, the case-law of the CJEU and the Supreme Courts of Member States such as Germany and France, has shown itself to be amenable to the possibility of applying the safe harbour under Article 14 of the DEC (*hosting*) to these search engines, provided that, in the case being heard, the role that the search engine adopts in the task being performed is deemed to be passive, technical or automatic.

This passive role -and, by extension, the existence of an exemption from liability is accepted almost unanimously with respect to the results yielded by the search engine on conducting a given search (natural results).

Furthermore, this exemption has also been allowed by CJEU case-law where the search-engine operator profits by establishing paid hyperlinks to content that infringes third-party rights (e.g., trademark rights). Hence, the obtaining of a financial reward is

not a criterion of direct exclusion of the safe harbour: instead, it is a factor to be borne in mind, along with other criteria, in order to decide whether, in a given case, the search engine continues playing a merely passive and automatic role vis-à-vis the content matter to which it directs end-users.

In other legal systems, however, the profit motive bars the search-engine operator from benefiting from the limitation of liability. This is what happens, for instance in Colombia, where the limitation for Internet search-engine operators is conditional upon their not receiving a financial profit *directly attributable to the infringing activity*. The same occurs in other countries studied, such as Rwanda.

In addition, there is wide-ranging agreement on the fact that, if the hyperlink provider has actual knowledge that the content to which it is directing the end-user is illegal, there is no sense in exempting it from liability. Not only is this specifically stipulated in all the jurisdictions studied (Spain, Chile, Rwanda and Morocco), but it has also been mandated by a series of court decisions in countries such as Italy and Germany, whereby such search-engine operators are deemed to be under an obligation to act, by removing the hyperlinks to illegal content when they become aware of such illegality.

In contrast, where such actual knowledge clearly does not exist or its existence is at least doubtful, the courts have for the most part shown themselves to be in agreement in declining to find liability.

Insofar as the liability of Internet search engines is concerned, the German Supreme Court has, moreover held that, with respect to content stored by the search-engine operator on its servers there is implicit consent on the part of the rightholder which excludes liability for copyright infringement.

In Belgium, in contrast, the appeal courts have deemed that, in line with the CJEU's decision in the *Infopaq* case, reproduction of the headlines and initial lines of newspaper articles in the results yielded by the search engine implies an act of partial reproduction of such articles, without there being any room in these cases to speak of the existence of implicit consent or authorisation. The same has occurred in some decisions of the lower courts in France and Spain.

It is also generally accepted that, in the case of search engines on pages that establish hyperlinks on an individual basis, the degree of knowledge or awareness of the illegal nature of the linked content is very different to that in the case of a web page which has a list of links to files containing copyright-protected literary or artistic works (referred to as "link-listing websites" in this paper).

5. Distributors of file-exchange programmes

In the case of persons who develop and commercially exploit computer programmes that enable files to be exchanged by means of P2P technology, there is an absence of legal regulation in this regard in most of the countries studied. Even so, in countries such as France and Italy, the law clearly establishes the illegality of the conduct of anyone who designs a programme manifestly aimed at enabling the exchange of protected works and makes it available to the public for the purpose.

In the case-law reviewed there seems to be consensus on the fact that it would be unreasonable to issue a blanket ban on the circulation of these types of programmes, which allow for totally lawful use in cases where the files exchanged do not infringe third-party rights.

In other cases, however, the point has also been made that the designers of these types of programmes cannot avoid incurring liability for contribution to the infringement (*secondary liability*), in cases where, in practice, their product almost exclusively serves to permit or facilitate the infringement of intellectual property rights, as has been held by some decisions in Germany.