Markt/2006/09/E
Service Contract ETD/2006/IM/E2/69

STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES

A. INTRODUCTION
B. RECOMMENDATIONS
C. GENERAL TRENDS IN EU

November 12th, 2007

Thibault Verbiest, ULYS

Prof. Dr. Gerald Spindler,
Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law
University of Göttingen

Giovanni Maria Riccio, University of Salerno

Aurélie Van der Perre, researcher at the CRID
Under the direction of the Professor Montero
University of Namur (FUNDP)

STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES

A. INTRODUCTION
B. RECOMMENDATIONS
C. GENERAL TRENDS IN EU

November 12th, 2007

Table of Contents

Markt/2006/09/E
Service Contract ETD/2006/IM/E2/69

STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES

A. INTRODUCTION
I. Scope of the Study
II. Method of the Study

November 12th, 2007

Thibault Verbiest, ULYS

Prof. Dr. Gerald Spindler,
Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law
University of Göttingen

Giovanni Maria Riccio, University of Salerno

Aurélie Van der Perre, researcher at the CRID
Under the direction of the Professor Montero
University of Namur (FUNDP)

I. SCOPE of the STUDY

A. Liability regime and development of E-Commerce

Directive 2000/31/EC on electronic commerce (hereinafter referred to as: "the directive") aims to remove obstacles to cross-border provision of on-line services in the Internal Market and to provide legal certainty to businesses and citizens. It was adopted on 8 June 2000.

Articles 12 to 14 of the directive establish precisely defined limitations on the liability of intermediary service providers who offer mere conduit, caching and hosting.

The study takes into account the fact that some Member States – motivated by the legitimate wish to provide for additional legal clarity - included in their transposition certain additional elements not covered by the directive, such as the liability of providers of hyperlinks, search engines or other intermediaries.

The liability limitations in the directive apply to certain clearly delimited activities carried out by internet intermediaries, i.e. to the technical process of access and transmission provision, as well as storage of information provided by a recipient of the service in a communication network. The liability limitations provided for by the directive are established in a horizontal manner, i.e. they cover civil, administrative and criminal liability for all types of illegal activities initiated by third parties online, including copyright and trademark piracy, defamation, misleading advertising, unfair commercial practices, child pornography etc. The liability limitations of intermediaries were considered indispensable to ensuring both, the provision of basic services which safeguard the free flow of information in the network and the provision of a legally certain framework which allows the Internet and e-commerce to develop.

Articles 12 to 14 of the directive do not affect the possibility for a national court or administrative authority to require a given service provider to terminate or prevent an infringement on a case-by-case basis (i.e. to issue injunctions aiming at removal of illegal information or the disabling of access to it) which is – in principle – subject to the national law of the Member States.

Article 15 prevents Member States from imposing on internet intermediaries, with respect to activities covered by Articles 12 to 14, a general obligation to monitor the information they transmit or store or a general obligation to actively seek out facts and circumstances indicating illegal activities. This is important, as general monitoring of millions of sites and

web pages would, in practical terms, be impossible and would result in disproportionate burdens on intermediaries and higher costs of access to basic services for users.

However, **Article 15** does not prevent public authorities in the Member States from imposing a monitoring obligation in a specific, clearly defined individual case (recital 47).

Articles 14 and 15 do not affect the possibility for Member States of requiring hosting service providers to apply duties of care which can reasonably be expected from them and which are specified by national law, in order to detect and prevent certain types of illegal activities (recital 48).

B. Liability regime and Notice and Take-Down procedures

The conditions under which a hosting service provider is exempted from liability, as set out in Article 14 (1) (b) of the directive, constitute the basis for development of notice and take down procedures for illegal information by stakeholders. As already mentioned above, Article 14 applies horizontally to all types of information. At the time when the directive was adopted, it was decided that notice and take down procedures should not be regulated in the directive itself. Instead, **Article 16 and recital 40** of the directive expressly encourage self-regulation in this field.

The study takes into account the fact that some Member States included in their transposition measures certain additional elements not covered by the directive, such as (statutory) notice and take down procedures for illegal content.

C. Aim of the Study

Article 21 of the directive requires the Commission to submit to the European Parliament and the Council every two years a report on the application of this directive, accompanied, where necessary, by additional measures in order to take account of legal, technical and economic developments in the field of information society services.

In November 2003 the Commission published a First Report on the application of the directive. Considering the lack of practical experience with the directive at that time the report concluded that proposals for complementary measures would be premature. No date has been fixed for the second report for which the current study will provide input.

This study should provide the Commission with accurate information relating to the application of the liability section of the directive (Section 4; Articles 12 to 15) in order to be able to evaluate the need for complementary measures in line with Article 21 of the directive.

Collection of information shall enable the EC to:

1. Carry out an analysis on whether the national case law is developing in conformity with the letter and spirit of the Section 4 of the directive.
2. Evaluate whether the self- and co-regulation in the area of notice and take down has been developing in line with the letter and spirit of the Section 4 of the directive.
3. Evaluate whether the national courts when making use of the possibility to require a given provider of information society service acting as intermediary to terminate or prevent an infringement are doing so in a manner compatible with the letter (in particular, Article 15 (1)) and spirit of the Section 4 of the directive .

The first objective of the study is to provide accurate information enabling evaluation of the impact of existing Community rules applicable to internet intermediaries (Section 4 of the directive) on the cross-border provision of these types of information society services.

Secondly, the study must provide accurate information enabling evaluation of the impact on the functioning of the Internal Market for intermediary information society services of existing national rules (legislative measures, case law, co- and self-regulatory measures) in the areas not (at least explicitly) covered by Section 4 of the directive with the view of the eventual need for further Community action in this area of the liability of internet intermediaries.

II. METHOD of the STUDY

A. Phases

The study is carried out in four phases.

In a **first and second phase**, the Study identifies and specifies the relevant significant case law, as well as all existing co- and self-regulatory measures providing for notice and take down procedures in all EU-25 Member States. Case-law and regulations are summarized in detail. Copies and translations (in English of French) are provided.

In the **third phase**, the Study evaluates whether certain trends are being developed in the area of regulation of the liability of internet intermediaries – across certain Member States or at the EU-25 level. The existing jurisprudence and self- and co-regulatory measures providing for notice and take down procedures are regrouped according to these trends.

In the **fourth phase**, the Study draws conclusions whether the existing national case law in the areas specified above, as well as the existing self- and co-regulatory measures in the area of notice and take down procedures are developing in due respect of the letter and spirit of the directive.

B. Scope of First and Second phase

In order to achieve the aim and objectives, it was decided to extend the list of Internet intermediaries to the current existing and practically effective categories of intermediaries. Are taken into account, Mere conduit, Caching, Host providers and Auction platforms, Search engines and Hyperlinks, Blogs and Forums, Content aggregators, Domain name providers and Registration authorities, Admin-C and online-payment providers, and Gambling specific issues.

1. The study firstly provides detailed updated information about the existing case law which provides for interpretation and application of the national measures transposing the liability section of the directive in all EU-25 Member States.

   The case-law focuses on:

   a. The definition of the intermediaries.
   b. The interpretation and application of exoneration conditions for the providers of information society services (such as interpretation and application of concept of

"awareness", "actual knowledge", "obligation to act expeditiously upon obtaining such awareness or actual knowledge" laid down in Article 14 (2) of the directive),

c. The technical statutory measures ordered by injunctions by public authorities in order to block or remove illicit contents.
d. Measures imposing specific monitoring obligations (in due respect of the prohibition of the general obligation to monitor enshrined in Article 15 (1) of the directive) and – if applicable – concerning measures imposing an obligation to promptly inform the competent authorities of alleged illegal activities undertaken or information provided by the recipient of the service in question and measures imposing an obligation to communicate to the competent authorities, on their request, information enabling the identification of recipients of their service with whom they have storage agreements in all EU-25 Member States (communication and cooperation obligations).

2. Secondly, the Study details up to date information about existing self-, co- and regulatory measures in the area of notice and take down procedures in all EU-25 Member States.

More specifically, this second part focuses on:

a. Codes of conduct and other agreements elaborated between various stakeholders in order to provide for notice and take down procedures for illegal (and harmful) information when one of the parties to such agreements is a provider of an information society service consisting in hosting (as provided for in Article 14 (2) and recital 40 of the directive) or a provider of another type of intermediary service.

b. Co-operation protocols and other agreements providing for notice and take down procedures for illegal (and harmful) information transmitted or stored which have been encouraged by Member States and/or to which the Member State in question is a party.

C. Structure of the Study

The third phase (General Trends in the EU) is presented in a self-standing paper containing the trends identified.

The fourth phase (Recommandations) is presented as a self-standing paper containing conclusions of the Study drafted as a text, coupled with the conclusions summarized in a PowerPoint presentation as a self-standing paper.

The third and **fourth phases** are also presented in this document beginning with the **Scope of the Study** and the **Methodology**.

The First and second phases are presented in annexes. These annexes contain, by country, a **Summary**, the **Report** of the relevant significant case-law, as well as all existing co- and self-regulatory measures providing for notice and take down procedures. These annexes also contain, if they are mentioned in the Report, **original language texts** coupled with **translations** into French or English. All the annexes end with a **list of abbreviations**.

The study and the opinions expressed in the report represent entirely the work of the Consortium and do not necessarily reflect those of the European Commission.

Markt/2006/09/E
Service Contract ETD/2006/IM/E2/69

STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES

B. RECOMMENDATIONS

November 12th, 2007

Thibault Verbiest, ULYS

Prof. Dr. Gerald Spindler,
Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law
University of Göttingen

Giovanni Maria Riccio, University of Salerno

Aurélie Van der Perre, researcher at the CRID
Under the direction of the Professor Montero
University of Namur (FUNDP)

RECOMMENDATIONS

A. Preliminary Remarks

The manner in which courts and legal practitioners interpret the E-Commerce-Directive ("ECD") in the EU's various national jurisdictions reveals a complex tapestry of implementation. This often reflects the distinct values found in each of the respective legal regimes. Moreover, changes in the social evaluation of the Internet (good or evil? enhancing communication or crimes and copyright infringements?), new techniques, and business models seem to have influenced legal practice and court decisions.

This report examines conclusions which might be drawn from case studies undertaken in the different member states. It also considers statements from various stakeholder groups (including those presented at a conference on liability provisions in the ECD, organised in Berlin in May 2007).

All of the proposals and suggestions in this report are made with due regard to the need to respect the existing legal framework established by various European Directives in this field, including those on InfoSoc[1], Enforcement[2] , and Audiovisual Media Services[3] Directives. It should be borne in mind throughout that there are few legal areas where the conflict between stakeholder groups is greater than that between copyright holders and the telecommunication and E-commerce industry. Balancing the conflicting interests will be a difficult task, and accordingly the proposals and conclusions presented in this report are provisional.

It should be noted that the conclusions of this report reflect exclusively the views of the consultants which do not necessarily correspond to those of the EU-Commission.

The conclusions herein focus firstly on the structure of the ECD and propose amendments, before concentrating on general problems which overlap all the different kinds of liability privileges, but remain largely unregulated by the ECD such as injunctions and information location tools (hyperlinks, search engines).

B. Mere Conduit

As regards the exemption from liability for mere conduit, there seem to be few problems concerning application and interpretation of the liability privilege regulated in Art. 12 ECD.[4] In contrast, court and administrative practice mainly had to deal with (administrative or civil

[1] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ 167/10 of 22.6.2001.
[2] Directive 2004/48/EC of the European Parliament and of the Council of 29.4.2004 on the enforcement of intellectual property rights, OJ 157/45 of 30.4.2004.
[3] The European Parliament has formally approved without amendments the Council's common position on the new Audiovisual Media Services without frontiers Directive, available at: http://register.consilium.europa.eu/pdf/en/07/st10/st10076-re06.en07.pdf.
[4] Cf. 3rd.Report Chapter C.I.

court) injunctions against access providers ordering for example the blocking of websites[5] as well as requests for information on names and addresses of recipients involved for example in copyright infringements (filesharing) etc..[6] Claims for damages or criminal prosecution against mere conduit providers apparently have not been important in practice.

However, the relationship between Art. 12 ECD and the telecommunication directives is still not very clear as access providers may be classified both as information service providers (according to the ECD) and telecommunication providers offering access to telecommunication networks (under the telecommunication directives). A closely related problem is the uneasiness in some member states about the range of mere conduits (or access providers). The *Paribas* case in France illustrates this point, applying access provider rules to a bank offering access to the Internet via its intranet. Moreover, new generations of mobile phones and the integration of different electronic and media services (convergence) illustrate the possible problems in member states in assessing services correctly – even if there are not yet any reported court cases dealing with the problem of qualifying certain services.[7]

Hence, it is not the current liability regime for mere conduit which causes difficulties, but rather the application of different data privacy regimes since there are still manifest differences between telecommunication data privacy rules (as in the Directive 2002/58/EC[8]) and those in the general privacy directive (Directive 95/46/EC[9]). This problem points at a more general issue: the technical convergence of services which are governed by different acts of community legislation. Whereas it is hard to resolve this issue in the context of this report it should be noted that the different regimes in the Audiovisual Media Services Directive, the Telecommunication Directives, and the ECD are increasingly confronted with problems of classifying convergent electronic services with overlapping characteristics. A general solution to these problems – already outlined in some of the directives – could be to concentrate on the function of a particular service (e.g. broadcasting via mobile phone) on the one hand or (alternatively) on substantive topics/legal issues, such as regulating liability for all electronic services regardless of their mass media character or of their qualification as telecommunication service on the other hand. However, it is beyond the scope of this study to evaluate the consequences and necessary criteria for developing a "catch-all" liability scheme able to cover all types of information and media services.

C. Caching

Concerning caching hardly any problems have arisen around the EU member states, so only a few court cases are reported. This is, in part, a result of the clarification provided by the

[5] Cf. 3rd Report Chapter D.II.4.a) (civil courts), D.III.2.a) (administrative actions)
[6] Cf. 3rd Report Chapter F.IV.
[7] Cf. 3rd Report Chapter C.I.
[8] Directive 2004/48/EC of the European Parliament and of the council of 29 April 2004 on the enforcement of intellectual property rights, OJ 195/16 of 2.6.2004.
[9] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31 of 23.11.1995.

InfoSoc-Directive in exempting temporary technical copies (ephemeral copies) from the requirement to be licensed. Only in some cases, such as access to the Usenet as a net of newsgroups (which uses mirroring to a large extent), has the liability exemption in Art. 13 ECD led to problems of interpretation since there are some doubts about the correct assessment of the facts concerning the definition of the service as caching.[10]

In practice some provisions of Art. 13 ECD seem to be "dead letter" law, such as the requirement of compliance with industrial standards ("rules regarding the updating information, specified in a manner widely recognised and used by industry", c. f. Art. 13 (1) lit. c ECD). There are hardly any industry standards in member states specifying these requirements – nevertheless, there seems to be no need to amend these provisions as legal practice tends to interpret them according to the customs and practices of a particular sector.[11]

D. Hosting

I. The definition of actual knowledge

Besides the general issue of how to classify a host provider[12] and the additional injunctions against host providers[13] there is one salient implementation issue with regard to host providers (Art. 14 ECD), this concerns the "actual knowledge" of a provider (and its required level of awareness) of facts and circumstances that suggest illicit content or activities (of third parties). National implementation and court practice differ between member states considerably when assessing actual knowledge. Some member states require a formal procedure and an official notification by authorities in order to assume actual knowledge of a provider, whilst others leave it to the courts to determine actual knowledge. A third approach is taken in some member states, offering two ways to determine "actual knowledge": a notice and take-down procedure, and the more traditional approach of notifying the provider according to the national legal standards of knowledge.[14]

At the centre of this problem is a conflict of interest:

- On the one hand, providers do not want to be entangled in the legal problems of their users/clients (in particular their dealings with third parties). Providers, as technical intermediaries, cannot always handle and assess complex legal matters. Whilst in some cases it might be easy to assess the illegality of contents or activities, such as those dealing with paedophilia, it is quite hard, even for lawyers, to tell if a trademark or a copyright has been infringed. Difficulties of legal analysis are exacerbated by the fact that traditionally intellectual property rights are demarcated according to

[10] See 3rd Report Chapter C.II., in particular the German decision LG München I, 19.4.2007, 7 O 3950/07, MMR 2007, 453, available at http://www.kremer-legal.com/wp-content/uploads/2007/04/lg_muenchen_i_7_o_3950_07.pdf.
[11] Cf. 3rd Report Chapter C.II.
[12] Cf. 3rd Report Chapter C.III.2. However, most court cases do not deal extensively with the definition of "host providers" under Art. 14 ECD.
[13] Cf. 3rd Report Chapter D.II.4.b), D.III.2.b)
[14] Cf. 3rd Report Chapter C.III.3..

territorial boundaries which are not always clear on the Internet. This raises difficult issues of conflict of laws (there are, naturally, some occasions where it is evident that a copyright has been infringed, such as in cases of sharing music or recently published movies). The same difficulties arise regarding defamation: The situation is aggravated by the fact that freedom of speech is one of the core elements of democracy, and providers can not exercise a judge-like role in order to assess the legitimacy of a statement. Moreover, given the large amount of information on the internet they cannot be compared to press publishers who can conduct at least marginal controls through employees prior to publications. Finally, if providers are to act upon mere notifications there could be potential abuse by fictitious "victims" seeking to hamper a competitor or adversary. This problem has already been acknowledged in the legislative motives concerning the Dutch implementation of the ECD which hold that a simple notification – like a message by anybody - is insufficient, whereas a court order always meets the requirements of a notice.[15] It is the interest of providers to act only upon "official notifications".

- On the other hand, it is in the interest of right holders (be it copyright holders or victims of defamation) and also in the public interest (in cases of paedophilia etc.) that providers act as fast as possible given the enormous potential of disseminating illicit content via the internet. Moreover, in most cases, techniques to camouflage a disseminator's identity render it easier for infringers to continue their illicit activities. It is hard for right holders (and the state) to enforce compliance with existing rules and norms. This is a result of the "anarchical" architecture of the internet - designed to circumvent breakdowns of elements of the net - which hinders effective control. In most cases it is only the provider who could be held responsible as the infringing parties are not known or are hard to reach – an issue that is also well known in the EU in the context of gambling sites due to different regulatory approaches in the member states.

II. Notice and Take-Down Procedures as a potential solution

To balance the competing interests noted above, two extremes should be excluded: mere reliance upon official notifications by authorities on the one hand and assuming actual knowledge following simple notification on the other.

- A focus on official notification may easily lead to a *de facto* exemption from liability of providers, even if they are clearly aware of illicit activities going on.[16] Official authorities often do not have the capacity or resources to pursue every infringement. As far as civil actions are affected, the likelihood of providers being sued could be very low, and enforcement will often be too late, even though those concerning copyright or trademark infringements are "better" enforced than other infringements (such as defamation).

15 See for more details 3rd Report C.III.3.c), in particular Country Report Netherlands.
16 For more details see 3rd Report C.III.3.c.) bb and in particular the Country Report Spain.

- Simple notification, on the other hand, would invite anyone to inform providers of contents or activities, regardless of the reliability, of the quality, and of the correctness of the notification. Even if the notifier could be held liable according to national legal systems, the probability of abuse is too high to accept a simple notification system. Moreover, simple notification places the burden of assessing the quality of the notification upon the provider. The provider is then confronted with the decision of taking down the content – even if it is legal – or facing the risk of being sued or being criminally liable. There is a greater likelihood that providers would take down content in order to avoid the risk of being sued or prosecuted rather that maintaining it. Exceptions to the rule against simple notification could be made for obviously illegal content which constitutes a severe breach of the public interest (such as in paedophilia cases or other crimes of a similarly disturbing nature).

One potential solution to this conflict could be the adoption of a modified notice and take-down-procedure combined with a counter-notice and put-back option. This has been implemented in Finland[17] and Lithuania[18]. Under such a system, it would be up to the right holder to notify the provider about the infringement. Having received the notification the provider would be required to act expeditiously in provisionally withdrawing the content and informing the customer about the notification. However, in order to avoid any contractual liability or criminal responsibility[19] these procedures should be supported by legal provisions to ensure that the provider does not incur any liability or responsibility as a result of sending a notification to its customer, be it a contractual liability or a tort (such as assisting the customer in abetting). This approach is already partially applied in Poland.[20] Under such a scheme, it would be up to the customer to make a risk assessment as regards whether he should send the provider a counter-notice. Only after receiving such a counter-notice would the provider be obliged to put back the content on-line. If the provider does not receive an answer from the right-holder indicating that he will file an action against the client the provider will be obliged to put the content again online; if the right-holder files an action against the client the provider is obliged to take down the content until the final decision of the court. This counter-notice system is in operation in Finland and in the US (operated by the Digital Millennium Copyright Act (§ 512 (g) (2) (C), DMCA)).

However, in order to avoid any abuse of this procedure member states should be obliged to introduce rapid preliminary review proceedings (as used, for example, in Germany) concerning unlawful competition or intellectual property rights infringements. Where a customer has sent a counter-notice to the provider (so that the content is again online) the provider should inform the right-holder immediately, allowing the latter the opportunity to file an immediate application for a preliminary injunction, probably without a hearing at first

---

17 Cf. 3rd Report Chapter H.I. and more details in Country Report Finland.

18 Resolution N° 881 « Concerning Acceptance of a Report on Provisions for Eliminating the Possibility of Access to Unlawfully Obtained, Created, Amended or Utilised Information", http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=303361&p_query=&p_tr2= .

19 As was suspected by Italian providers, for more details cf. the italian country report.

20 Cf. 3rd Report Chapter C.III.3.c), more details in Country Report Poland.

instance. This would provide right-holders with an opportunity to protect themselves. Equally, providers would not be placed in the invidious position of having to act as *de facto* judges. Moreover, the risk of abuse – in particular the danger to freedom of speech – is largely reduced as the right-holder may well be entitled to file an action for injunctive relief.

The notification could follow certain rules, as provided for in French legislation, such as requiring the name and other details of the person tendering a notice and identifying specifically the incriminating content. To avoid any bureaucratic procedures, providers could be obliged to publish corresponding templates on their websites – as France already requires and most providers do.[21] Whilst the design of such a template could be left to self-regulation, an agreed European template would be preferable in order to avoid a situation where victims have to incur costs in order to inform themselves about the different procedural requirements on each occasion.

An exception to the above-mentioned scheme should be applied where the public interest is concerned (again following the model in Finland): Given the fact that the illegality of some activities or content is easily assessed, even by laymen and non-lawyers, there should be a catalogue that lists all content which is not subject to a notice and take-down procedure. In these cases, any awareness of the provider – even by way of simple notification – should be sufficient to trigger its responsibilities.

E. Information Location Tools

As the ECD deliberately left untouched the liability regime for hyperlinks and search engines it is not surprising that most member states have developed different rules to cope with this issue.[22] However, these rules vary, as does court practice[23] (which, however, seems widely to exempt information location tools from liability). information location tools are one of the core elements of the internet and of modern electronic communication networks; there is therefore need for European harmonization. In contrast to other issues, there appears to be a potential consensus amongst stakeholders:

I. General reflections

There are certain considerations which should be taken into account and acknowledged when dealing with information location tools:

- Information location tools generally serve a social need, as they facilitate internet use (and that of any other electronic network) – as has been explicitly acknowledged by some courts in member states such as the German Federal Court.[24] This is true for search engines as well as for hyperlinks. Since information location tools are of social value, constraints on their use should be particularly justified and well-founded.

---

21 For details cf. 3rd Report Chapter C.III.3.bb), in particular Country Report France.

22 Cf. 3rd Report Chapter G.II.2.a) (search engines), G.II.3.a) (hyperlinks).

23 Cf. 3rd Report Chapter G.II.2.b), G.II.3.b)

24 See for details 3rd Report Chapter G.II.2.b) (search engines), G.II.3.c) (hyperlinks). in particular Country Report Germany.

- Liability exemptions should take into account the different levels of control and of awareness that a provider of information location tools has concerning the content to which the tool directs the user. In other words, it is hard to control the web-sites to which a user is directed by using a search engine, not least because a search word may be used in several different contexts. An obligation to check and verify the contents of web-sites identified by a search engine would lead, ultimately, to an obligation to perform a manual review– which would hamper the automatic indexation of the web and significantly reduce the amount of information that is accessible. However, the degree of control required may vary in the future as a result of technical developments (e.g., such as indexing web-sites according to their level of respect of measures aimed to protect minors or data-protection safeguards). If the provider of the information location tool has actual knowledge of illicit activities or content to which the tool is directing users there is no reason to exempt it from liability. If, for example, a setter of a hyperlink is clearly aware of the fact that the website to which the hyperlink directs the user contains illicit content he facilitates for others the access to the illicit content and increases its dissemination. On the other hand, knowledge of illicit content can only be assumed if the link (or the search engine reference) leads the user directly to the incriminating web-site – and not merely to a root page which would then enable the user to find the incriminated web-site. In other words, setters of information location tools cannot be held liable for indirect infringements .
- Another exception to the general rule of exemption from liability should apply in the case of abuse: providers should be held liable if they advertise their information location tools with specific reference to illicit content, such as centres for hyperlinks directed exclusively to such material.[25] Whilst it is not easy to make out the precise borderline as to where abuse begins and ends, it is a generally accepted legal principle that circumvention and intentional abuse should not be granted liability exceptions. Such an approach reflects the arguments developed by the US Supreme Court (in the *Grokster* case),[26] and followed by some courts in European member states (such as the Hamburg Court of Appeal[27]).

In light of these general reflections, rules should depend upon the degree of control and on actual knowledge:

II. Hyperlinks

Some member states provide for hyperlinks an explicit liability exemption modelled closely on those for host providers.[28] This seems appropriate, as it takes into account that the setter of

[25] As the case in Belgium when users could upload hyperlinks directing them to pornographic websites and the hyperlink centre was explicitly dedicated to such use, Cassation, 3 févr. 2004, *R.D.T.I.*, 2004, n° 19 ; En première et seconde instance : Corr. Hasselt, 1er mars 2002, *inédit* ; Anvers, 7 oct. 2003, *A.M.*, 2004, liv. 2, pp. 166 et s., for more details see the country report on Belgium.

[26] US Supreme Court, MGM Studios v. Grokster, 125 S.Ct.2764, 162 L.Ed.2d. 781

[27] OLG Hamburg 8.2.2006 – 5 U 78/05 – Cybersky, available at http://www.jurpc.de/rechtspr/20060029.htm (German), for more details see the German country report.

[28] Cf. 3rd Report Chapter G.II.3.a).

a hyperlink is regularly aware of the content of the website to which he is directing users via his hyperlink. In other words, unlike search engine operators like Google which conduct mere automatic searches without taking notice of the search results at all, the placing of a hyperlink is a deliberate action by the person setting the hyperlink. However, the setter of the hyperlink cannot be held liable for changes to the linked web-site *after* he has set the link since he is not in a position to obtain knowledge of such changes (unless he is notified of modification, via the NTD-procedure). Again, any circumvention or abuse should not fall under the liability exemptions.

Such a liability exemption allows for a balance to be struck between the service provided by hyperlinks and need to prevent unlawful activities.

III. Search Engines

In considering search engines, a distinction must be drawn between so-called "natural results" or simple references (i.e. automatically generated links to web-sites as the result of a search) and so-called "commercial links" (or "Adwords") which are used by search engine operators in order to generate revenues via a personalized advertisement system:

1. "Natural results" – Simple references

With regard to "natural results", the social benefits of search engines outweighs all the disadvantages resulting from the listing of unlawful content amongst other material. Hence, search engines could be compared to access providers – indeed, some member states have acknowledged this by conferring on search engines the liability exemption contained in Art. 12 ECD.[29] The above-mentioned exceptions to the general rule (in particular regarding abuse) can also be addressed by a clause concerning circumvention or abuse – the existing provisions in Art. 12 ECD with regard to collusive behaviour or selection of contents/addressees of content which is transmitted do not encompass this type of abuse, such as search engines exclusively programmed to refer to illicit content (e.g. child pornography search engines). Alternatively, search engines could be treated like host providers.

With regard to search engines as with any other type of intermediary, the core issue is not liability for damages, but injunctions ordering the blocking of illicit search results and the prevention of the future display of those search results. Injunctions might almost lead to specific monitoring obligations (to be practically implemented, for example, by filtering). These problems will be addressed in a broader context, cf. F below.

2. Commercial links – Adwords

Another field of interest concerns the use of commercial links or adwords. This has been a particular issue in France and Germany.[30] However, it is hard to conceive of liability exemptions in a system that is designed to generate revenues for the search engine operator and which is, in principle, controlled by the search engine operator. As far as these systems

29 Cf. 3rd Report Chapter G.II2.a).

30 Cf. 3rd Report Chapter G.II.2.c)

are concerned, the reason for exempting providers from liability is not applicable, as providers do not act as mere technical intermediaries. In contrast to court decisions[31] that have relaxed liability for trademark infringements for domain-registrar systems due to their non-profit-character[32] the adwords/commercial link system of search engine operators is clearly profit orientated. Hence, as search engine operators can have recourse to legal action against their clients (who infringe trademarks for example) by prohibiting certain action in their contractual terms of business, there is no reason to shift the risks of trademark infringements to right holders. However, note that the question if the use of search word by an adword system itself constitutes a trademark infringement is not resolved and left to trademark law.

F. Injunctions and Filtering

Injunctions – and closely related filtering and blocking – are one of the outstanding problems in the EU to be left untouched by the ECD.

The issue of injunctions is slightly different from the problems discussed above concerning the conflict of interests between right holders and providers. Whereas for the purpose of avoiding liability for damages and terminating identified infringements a NTD procedure might lead to satisfying results, injunctions concern the conflict between general monitoring by providers – which is widely held to be unfeasible – and the interests of right-holders not to be confronted by the same infringements again. In other words, injunctions refer to the prevention of infringements and future damages, which can not satisfyingly be achieved by a notice and take-down procedure.

There is much unease across EU member states regarding the scope of injunctions and measures necessary to filter and to block access to illicit content. Injunctions do not only concern host providers but also access providers or providers of information location tools. Injunctions pose certain common problems:

- First, it is hard to definitively assess and lay down the feasibility of techniques to filter and block. Injunctions have a dynamic character as obligations resulting out of the injunction concern a (specific) monitoring in the *future*. Hence, obligations (if at all) should meet industry standards that are widely accepted at the moment the injunction is handed down as the law cannot force a provider to undertake measures which are not feasible. Some courts obviously do see filtering techniques as feasible, as in the Belgium SABAM/Scarlet case. Other courts, like the Dutch in the Stokke/Marktplaats case, have considered alternatives for right-holders to pursue infringements by direct action against infringers, reasoning that providers are not able to filter efficiently.[33]

---

31 ´Cf. 3rd Report Chapter G.II.2.b), for Germany, cf. BGH, 17.5.2001, I ZR 251/99, MMR 2001, 671 (674) – ambiente.de

32 These systems work in a similiar way by offering domain names to interested parties in an automatized manner.

33 Cf. 3rd Report Chapter D.II.2, D.II.4., D.IV:

- Moreover, incentives for providers to develop filtering techniques largely depend on their capacities to do so. This may vary according to their character as a profit- or non-profit-making-organization. In other words, a private website-owner without any profit interest (and without resources) cannot be expected to be able to develop filtering techniques on his own.
- Closely related to the assessment of filtering capacities is the unresolved issue of who should be obliged to produce evidence that filtering techniques are being used - providers or right holders? Economic efficiency theory indicates that the cheapest cost avoider is the party who is "nearest" to the technical information and can therefore best control and manage it. It follows that the burden of proof should lie with that party. Hence, it should be the provider who is required to adduce evidence that filtering techniques do not exist. Since this evidence may be hard to produce, citation of widely accepted industry standards[34] could serve as a *prima facie* proof - as in other legal areas such as product safety or product liability
- One problem, (which seems specific to Germany but is emerging in other member states such as France and Italy) is the extent of the infringements that can be covered by injunctions.[35] Whilst right-holders have a strong and legitimate interest to ban not only specific illicit content (or infringements) but rather all similar infringements in the future, providers are confronted with the problem that they cannot monitor all similar content. Assuming that there are no filtering techniques available to manage and control similar infringements, such an obligation would result in an overall monitoring obligation. However, this depends largely on the availability of filtering techniques. This issue is at the centre of all legal attempts to find a balance between providers' liability (in Germany: "accessory liability"[36]) and their capacity to filter illicit contents (see, for example, the German notion of proportionate obligations to examine content in advance).
- In France, Article 6.I.8 LCEN[37] stipulates a principle of subsidiarity for injunctions « *The legal authority may order as an emergency interim ruling or on request, any person cited in paragraph 2 [Host provider] or, in their absence, any person cited in paragraph 1 [Access provider], to take all measures liable to prevent damages or to cease damages caused by the content of an online public communication service* ». In the Aaargh case[38], the access

[34] Such as CEN-Standards though these not yet have been adopted.
[35] Cf. 3rd Report Chapter D.I.3., D.II.2.
[36] For the concept of „accessory liability" in German law see 3rd Report Chapter D.I.3, D.II.2.. and the German Country Report.
[37] LCEN, Loi n° 2004-575 du 21 juin du 2004 pour la Confiance en l'Economie Numérique, www.legifrance.gouv.fr
[38] TGI Paris, 20/04/2005, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, http://www.juriscom.net/documents/resp20050627.pdf

> providers asked the judge to verify first of all whether the host providers had complied efficiently with the court order before ordering injunctions against the access providers (the injunction for filtering had been ordered without any precise technical precept and without any time limit). The Court of Appeal confirmed that the principle of subsidiarity was well applied. The Supreme Court (Cour de Cassation) has been appealed to by the access providers and, if called upon, will certainly give the precise details of the mechanism of subsidiarity according to the LCEN.[39]

To strike a balance between the interests of the parties is difficult. The starting point should be that providers will be given an incentive to develop and use filtering techniques in order to ban similar infringements in the future. However, they should not be held liable for the general absence (non-availability) of technical means to avoid such infringements. The availability of filtering techniques may vary largely according to the content to be monitored, such as coyprighted contents or defamatory speech.

To solve this dilemma there are multiple possibilities. One solution could be to rely upon the principle of negligence in civil law (not strict liability) and leave it to the courts to develop criteria. However, this might lead to a fragmented European scene of different standards, exemplified the contrasting decisions of the German Federal Court and the Dutch court concerning operators of market platforms.[40] Moreover, there is no guarantee that a balanced and dynamic standard would be established in time and provide legal security for both sides. It would be left to the courts to define these standards. There would be no guarantee at all that relevant cases would be brought before the courts allowing for the establishment of these standards.

We would therefore submit that a mixed co-regulatory model, making reference to the model in Art. 13 ECD, and referring to industry standards, may be used, perhaps restricted to some (prominent) sectors such as copyright or trademark infringements (such as in Finland for NTD-procedures). In order to avoid a situation where no standards were developed (and instead customary practices were applied) the model could be enhanced by adding elements from EU product safety models (so-called "New Approach"), such as mandating European standardization committees (CEN) to develop standards. Stakeholders like right holders could participate in these standardizing committees along with providers. Thus, dynamic standards and legal security could be ensured, since courts would have to respect those standards. Under such a scheme, only where filtering techniques according to those standards were available

---

TGI Paris, 13/06/2005, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf
CA Paris, 24/11/2006, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf

[39] More details in 3rd Report Chapter D.I.2.

[40] See the case Internet-Versteigerung I (ricardo.de), Internet-Versteigerung II in Germany (details in the Country Report Germany) on one hand and the Stokke/Marketplaats case on the other (details in the Countrx Report Netherlands).

could providers be ordered to filter and block similar infringements. This would still leave enough leeway for providers to develop their own technical solutions – technical solutions of individual providers deviating from the recognised standards would not be prohibited. However, when deviating from standards the onus of proof regarding the equivalence of individual technical measures and specifications in standards would lie upon the provider.

The same model could be applied in other areas such as online press (discussion fora, blogs etc.). There are already self-regulating bodies in place here, as in Germany. These (or other) bodies could develop standards which are to be followed by providers in cases of defamatory speech. Alternatively, in order to take into account specific circumstances of defamatory cases etc., which might be quite different from copyright infringements, the assessment of obligations could be left to court practice.

Finally, such a model could be combined with incentives for providers to comply with these standards by giving right-holders the right to claim for broad injunctions. In other terms, only providers who complied with industry standards could invoke such a defence (injunction limited to a specific content) - others would face comprehensive filtering injunctions.

Finally, providers without any interest in generating profits out of their activities should be exempted from these rules. Their obligations should be restricted to filter specific contents only.

G. Communication obligations – Actions to disclose information

Another area of conflict concerns obligations to communicate and disclose information about users and clients. However, as these obligations are deeply connected to privacy directives on one hand and intellectual property rights directives (such as the enforcement directive) on the other this report will refrain from discussing these issues further. In any case, the European Court of Justice is about to give a decision on this.[41] A mere change in the ECD would not be sufficient to resolve this particular conflict.

H. Web 2.0 – Content aggregators etc.

As far as Web 2.0-services or content aggregators are concerned, we submit that it is necessary to wait further developments. As a general rule, it is unwise to adopt legal rules relating to business models of a possibly ephemeral nature. The ongoing development of web 2.0-services is too multifaceted to be reduced to one model. Moreover, the existing rules seem to be appropriate: questions of liability could be judged according to degree of content control, selection of contents etc. – all criteria that are already in place and could be handled by courts.

[41] Conclusions of the Advocate General Juliane Kokott of 18.7.2007, Case C-275/05, Productores de Música de Espana (Promusicae) v Telefonica de Espana SAU.

I. Other issues

Some stakeholders have complained about fora shopping in the EU, at least in Germany. However, this phenomenon is closely linked to the European Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters[42] and cannot be changed by the ECD – which has deliberately declared that it does not intend to address issues of jurisdiction. Hence, we leave this issue aside.

[42] Official Journal L 012 , 16/01/2001 P. 0001 - 0023

Markt/2006/09/E
Service Contract ETD/2006/IM/E2/69

STUDY ON THE LIABILITY OF INTERNET INTERMEDIARIES

C. GENERAL TRENDS IN THE EU

November 12th, 2007

Thibault Verbiest, ULYS

Prof. Dr. Gerald Spindler,
Department of Civil Law, Commercial and Economic Law, Comparative Law, Multimedia- and Telecommunication Law
University of Göttingen

Giovanni Maria Riccio, University of Salerno

Aurélie Van der Perre, researcher at the CRID
Under the direction of the Professor Montero
University of Namur (FUNDP)

I. SUMMARY

Some trends are salient throughout EU member states:

- Injunctions against providers and orders to filter and block illicit content
- Different treatment of actual knowledge (article 14 ECD)
- Divergent handling of information location tools (search engines, hyperlinks)
- Actions against providers to disclose customers' data in order to pursue (copyright) infringements

Pre-eminent amongst all cases are claims for **injunctions** against access providers and host providers. Most injunctions concern copyright infringements; however, it must be noted that the terminology and legal treatment of "injunctions" seem to vary widely across the EU: Most member states treat injunctions as some kind of preliminary relief for right holders, but others treat injunctions as a legal remedy *sui generis*, giving the right holder a claim to prevent future infringements in general. Besides copyright or trademark infringement cases there are also some injunctions ordered by public authorities (as in Germany, France or Italy) addressing the blocking of access to racist content, child pornography or foreign gambling activities.

One heavily debated issue in connection with injunctions is the feasibility of filtering techniques, either from a mere technical point of view or from a legal perspective with regard to freedom of speech as well as a balance of interests (costs and benefits). Only one court (Belgium SABAM/Scarlet) has handed down an order to an access provider obliging it to make use of a certain filtering technique. Other courts rely upon other criteria, such as provoking illicit content (in case of defamation in an internet discussion forum/Germany) or an analysis according to specific circumstances (Germany – auction platforms). Some courts (as in the Netherlands) deem a notice and take-down procedure as sufficient to fulfil the "duty of care" obligations of a provider (a market platform operator).

Another trend concerns different approaches to the notion of "**actual knowledge**" (of Article 14 ECD). Some member states (like Spain) consider only notifications by competent authorities as sufficient to assume actual knowledge. Courts in other member states (like in Germany or Austria) refer to general legal standards of obtaining knowledge of illicit content. A third group of states might be characterized by the Finish approach which relates "actual knowledge" to a formal notice-and-taking-down procedure but restricts it to copyright infringements. As to other content, Finland applies more general legal standards.

I**nformation location tools** are handled differently across member states. Some states apply the liability exemptions for access providers to search engines whilst others apply general principles of law. For hyperlinks, some member states codify liability exemptions - following the rules for host providers - whilst others apply general principles of civil or criminal law, differentiating between various kinds of hyperlinks and criteria of social usefulness.

One outstanding issue concerns the "adwords" system which is being used by some search engines operators in order to generate revenues by providing special links (so-called "commercial or sponsored links") whenever a specific "adword" has been used by a user. Whereas some courts (as in France) do not assign any liability exemption to the operators of search engines courts in other member states (as in Germany) apply the general rules on liability (contained in the civil code) in order to hand down preventive injunctions. In the latter case courts have emphasised the automated sale of adwords whereas the former approach stresses the fact that "adwords" are used by the search engines for their own purposes.

Finally, there is a substantial trend towards **claims for disclosure of information** by host or access providers of their customers' data. Again, court practice varies widely: Whereas UK courts do grant such claims and do not see any hindrances on grounds of privacy, other courts, such as those in Germany or the Netherlands, have rejected such actions. The issue will be resolved by a pending case before the European Court of Justice (ECJ).[43] Closely related to these claims are some acts in member states that impose a general obligation for providers to inform authorities about illicit activities, sometimes combined with an obligation to block or filter certain websites which are named in a catalogue issued by a state authority (as in Italy concerning gambling activities or for child pornography).

Self- or **co-regulatory approaches** are used across EU member states in different ways: whereas some providers have introduced a European wide program for a notice-and-take-down-procedure other member states scarcely report any self regulation by industry/providers. Some member states have codified a notice-and-take-down-procedure, as in Finland or in France (where it is optional).

[43] Case C-275/05, Productores de Música de Espana (Promusicae) v Telefonica de Espana SAU.

II. REPORT

Preliminary Remarks

The volume of reported case law and academic discussion concerning the Electronic Commerce Directive ("ECD") varies widely across EU member states. This is, in large part, due to the fact that some member states have only recently implemented its provisions into their national legal regimes. Not all national courts have had an opportunity to clarify and interpret the terms used in their national law. Some cases reported stem from a period when member states had not yet implemented the ECD liability regulations and when liability exemptions for internet service providers (ISP) were largely unknown. However, this pre-ECD case law cannot be neglected, as it may continue to influence the approach taken by some member state courts.

Moreover, it should be noted that there are still significant discrepancies between the legal cultures in each EU member state, given their different sources of general civil and/or criminal law. A member state's approach to the issue of providers' liability is often based upon a general doctrine of contributory liability - rendering the horizontal liability exemptions provided for by the ECD difficult to implement. One important example of where national legal traditions have a significant impact on the application of the ECD is the differing interpretations of the key notion of "actual knowledge". These inconsistencies are most apparent when comparing civil and criminal law approaches to contributory liability. Furthermore, a pan-European terminology for some services and providers is still missing - such as for "search engines" and "hyperlinks" - hampering a comparison between different jurisdictions. This report follows the "functional approach" in legal comparative research which is widely accepted by the international academic community.[44]

This report identifies common trends and crucial differences in the way that member states assess notions and concepts of liability for ISPs. It addresses some unique national trends which can not be observed in other member states, yet. These trends which are still specific for only just a few member states are important since they might be considered as a "blue print" for other member states when confronted with similar issues in the future.

The report on common trends uses a matrix structure: first, the focus will lie on court cases which are referring to the different liability provisions of the ECD, such as mere conduit, caching, and hosting. Second, the report will concentrate on recent trends (court practice) in member states which are not based on the liability regulations of the ECD but which have nevertheless an important impact on electronic commerce/services such as internet auctions,

[44] The "functional approach" assesses primarily the function of a specific norm regardless of its national categorisation. Thus, for example, a contractual liability norm could serve the same purpose in one state as a tort liability norm in another state.

hyperlinks, or search engines. It is evident that some repetitions and cross references are necessary for the sake of transparency.

The report is based upon the information given by the country reports, in particular the reported cases.

It should be noted that the conclusions of this report reflect exclusively the views of the consultants which do not necessarily correspond to those of the EU-Commission.

Part 1: National Legislation and Case Law

A. Interpretation of the Liability Exemptions

I. Mere Conduit (article 12 ECD)

The majority of member states have followed a *verbatim* transposition of Article 12. Some member states (such as Poland) intend to amend their implementing legislation in order to bring it more closely into line with the ECD's provisions.[45]

Most of the reported court cases concern injunctions which have to be addressed separately.[46] Only in one case, a French court (Court d`Appel) applied the liability exemption for mere conduit to a case of contractual liability of an access provider. The access provider could not provide TV access to his client as promised in the contract because France Telecom had given wrongful information concerning the abilities to receive TV.[47] There are scarcely any reported cases concerning the notion of a "mere conduit" and the criteria which render an access provider as being so categorised. Only in **Germany**, **France** and **Poland** the debate centres on the distinction between telecommunication services and information services, as telecommunication services are excluded from liability exemptions assigned to internet intermediaries.[48] The following cases on this issue are therefore noteworthy: A **French** court has defined an access provider as "someone who offers an access to an online communication service".[49] However, the exact scope of this interpretation remains unclear: The *Cour d'appel de Paris* qualified[50] a bank as an access Provider (before the ECD had been implemented into French law) which has not been contradicted by other French courts, yet. The case concerned the obligation of the bank to keep identification data and to communicate it to the authorities. The court argued that the bank gave access to other communication networks like the internet. **German** courts have only recently developed criteria to assess the notion of a "mere conduit". In one case a provider who allowed for access to the so-called "Usenet" was held not to qualify as a mere conduit - opting to categorise it as a caching provider (pursuant to Article 13

[45] See Polish Report Particle 1 B I, Act of July 18, 2002 on provision of services by electronic means (APSEM), Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (Dz.U. z 2002 roku, Nr 144, poz. 1204).

[46] Cf. below Part 1:B.II.4.a).

[47] FR4. – CA Paris[47], 04/11/2005, Free, inédit http://tabaka.blogspot.com/2006/01/responsabilit-de-plein-droit-un.html .

[48] See Country Report Germany Part. 1, B. I., Country Report France A.1. (and the Paribas Case), Country Report Poland Part. 1, B. I.; further details on the discussion in Germany can be found in *Spindler*, CR 2007, 239 (241); *Roßnagel*, NVwZ 2007, 743 (745); *Hoeren*, NJW 2007, 801 (802); *Spindler*, in : Spindler/Schmitz/Geis, § 2 TDG Rn. 22 ff.; *Schuster*, in: Beck'scher TKG-Kommentar, § 3 TKG Rn. 47 ff.; *Säcker* in: Säcker, § 3 TKG Rn. 38 ff..

[49] TGI Paris, 25/03/2005, www.forumInternet.org/telechargement/documents/tgi-par20050325.pdf .

[50] FR 5 - CA Paris, 4 février 2005, SA BNP Paribas c/ société World Press Online, http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=867 .

ECD)[51]. A contradictory ruling was delivered by another German court, which concluded that a provider - in similar circumstances - was in fact a host provider.[52]

II. Caching (article 13 ECD)

The vast majority of member states have carried out more or less *verbatim* transposition of Article 13 ECD in their national implementing legislation. Only a few member states have substantiated Article 13 ECD. **Cyprus**, for example adopted Act N° 156(I)/2004 of 30/04/2004, concerning the use of memory in routers (requiring a renewal of content each millisecond). The Cypriot legislation was also influenced by article 5(1) of the InfoSoc-Directive.[53] In **Lithuania** the Act (Law of the 25/05/2006 on information society services)[54] states that where information held in cache memory has to be modified for technical reasons (so that the substance is unchanged but the "technical envelope" is different) the liability exemption still applies. **Malta** deviates from the terms of the ECD by restricting its liability exemption for caching providers to liability for damages and excluding criminal responsibility.[55]

In court practice across member states the liability exemptions incorporating article 13 ECD concerning caching have not been of great importance. Although only a few cases appear, at first sight, to be clearly related to Article 13 ECD a closer examination reveals that this is not strictly the case. A recent high profile case concerned an action brought by Copiepress against Google in **Belgium**, alleging copyright infringement through Google's publication of news articles published by third parties (newspaper publisher etc.) and which had been copied by Google's cache system and made accessible to its users. The central issue in the case did not address temporary storage (necessary for the page indexation or for the enhancement of communication as envisaged by Article 13 ECD) or liability arising out of the actions of a third party, but rather Google`s own infringements (by copying third party content). The Belgian litigation concluded with the court[56] rejecting the application of e-commerce liability exemptions.

In another recent case, the **German** Regional Court of Munich I (Landgericht – LG) qualified an intermediary who provided access to the so-called "Usenet" (a specific newsgroups net inside the internet without any controlled structures) as a caching provider, since information of these newsgroups had been mirrored and stored on its servers for about 30 days. From the

[51] GE4. – LG München I, 19/4/2007, 7 O 3950/07, MMR 2007, 453.
[52] LG Düsseldorf, 23.5.2007, 12 O 151/07, available at http://webhosting-und-recht.de/urteile/Landgericht-Duesseldorf-20070523.html. See Country Report Germany Part. 1 C. II..
[53] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ 167/10 of 22.6.2001.
[54] Law N° X-614. This law revokes the previous ordinance about some information society services N° 119 of 10/04/2002.
[55] § 20 Electronic Commerce Act (Chapter 426) of 10 May 2002 (Act No. III of 2001, as amended by Act No. XXVII of 2002).
[56] BE7. – Tribunal de première instance de Bruxelles, 13.2.2007, www.droit.be, (CopiePresse c. Google); see also precedent rulings: BE15. – Tribunal de première instance de Bruxelles (cessation), 5.9.2006, www.droit.be, n° 2006/9099/A, (CopiePresse c. Google); BE16. – Tribunal de première instance de Bruxelles (opposition), 22.9.2006, www.droit.be, (CopiePresse c. Google).

court's perspective, the provider had not acted as an access provider but rather as a caching provider, enhancing and enabling its user's communications.[57] However, in a similar case, LG Düsseldorf qualified the provider of Usenet access as a host provider in circumstances where it had advertised storage times of "more than 30 days" (for content including attachments like MP3s - so-called binaries) and offered the content for downloading.[58] Similarly a **British** court accepted that British Telecom (BT) hosted Usenet newsgroups in the case Bunt v. Tilley[59] where newsgroup postings had been stored for a period of time, usually amounting to a few weeks, to enable BT's users to access them.

III. Hosting (article 14 ECD)

1. Differences in Implementing Article 14 ECD

The majority of member states have carried out near *verbatim* transposition of Article 14 ECD into to their national legal system. They distinguish between actual knowledge and, as regards civil liability for damages, awareness of facts or circumstances from which illegal activity or information is apparent.[60] In those member states, intermediaries may be held criminally liable only where they have actual knowledge, whereas civil liability for damages is subject to the lower threshold of an "awareness of facts or circumstances from which the illegal activity or information is apparent".[61]

Some member states have deviated slightly from the wording of the directive. The **Dutch** implementing legislation stipulates that a provider would not be liable for damages where it "cannot reasonably be expected to know of the illegal nature of an activity or information" (Article 6:196c (4) Civil Code), whereas according to **Portuguese** law, civil liability "shall still remain whenever, relating to known circumstances, the service provider should be aware of the illegal character of the information".[62] The **German** law Telemedia Act (Telemediengesetz - TMG)[63] also slightly deviates from the ECD by using the word "knowledge" instead of "actual knowledge". It has also to be noted that Article 5(1b) of the **Czech** Act no. 480/2004 Sb. (Certain Services of Information Society Act) requires receipt of *provable* information not just on the quality of the content but also as regards its illegal nature.

---

[57] GE4. – LG München I, 19/4/2007, 7 O 3950/07, MMR 2007, 453, http://www.kremer-legal.com/wp-content/uploads/2007/04/lg_muenchen_i_7_o_3950_07.pdf

[58] LG Düsseldorf, 23.5.2007, 12 O 151/07, MMR 2007, 534 (535), http://webhosting-und-recht.de/urteile/Landgericht-Duesseldorf-20070523.html.

[59] UK1. – Queen's Bench Division, 10/3/2006, [2006] EWHC 407 (QB); [2006] 3 All ER 336; [2006] EMLR 523, Bunt v Tilley & Others

[60] Austria, Belgium, Cyprus, Denmark, Estonia, France, Germany, Greece, Ireland, Italy, Lithuania, Luxembourg, Portugal, Slovenia, Sweden, United Kingdom.

[61] Germany, Italy, Portugal. See for the debate among legal scholars in Italy *Giovanni M. Riccio*, La responsabilità civile degli internet providers, Torino, Giappichelli, 2002; *Francesco Di Ciommo*, Evoluzione tecnologica e regole di responsabilità civile, Napoli, ESI, 2003.

[62] § 16 Law- Decree No. 7/2004 of 7 January 2004 (Diário da republica I-A n° 5 de 7/1/2004 p. 70.

[63] Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG) of 26.2.2007, BGBl. I, S. 179.

Other member states have taken a different approach by not providing for a distinction between actual knowledge and awareness of facts and circumstances and as regards criminal or civil liability.[64] Under **Latvian** law a host provider is exempt from liability if it does not have access to data, which "may indicate illegal activities or information".[65] **Hungary** and **Malta** apparently restrict their liability exemption for host providers to civil liability, excluding criminal liability.[66] **Hungary** is about to amend § 10 ECSA[67] in order to make clear that the liability exemptions also apply to criminal cases. It has been suggested that the wording„ liable for the damage caused by the content of information "should be changed into the more general term "shall not be responsible for the information".

Slight deviations in the incorporation of the ECD can also be found with regard to the obligation to remove or disable access to unlawful information (article 14(1) lit. b ECD). **Lithuania** provides for an obligation on the part of host providers merely to disable access to the offending content, but does not also required that it be removed[68]; the same position applies in Poland[69] and Finland[70]. By contrast, the **Slovak Republic** has only implemented an obligation to remove illicit information, but not to disable access.[71] **Sweden** has chosen a more general approach, requiring host providers to "prevent further dissemination" of illegal contents.[72]

Finnish law[73] establishes that a host provider will not be liable if it disables access to illicit content after receipt of either a court order, or (in cases of copyright infringements) a notification (within the context of the notice and take-down procedure) or if it has otherwise been made aware that the hosted content is apparently contrary to certain sections of the Finnish Penal Code (chapters dealing with child pornography, violence, bestiality, etc).

In addition to the regulations provided for in the ECD, **Cyprus** introduced a regulation which obliges host providers to stop providing hyperlinks to illicit contents (section 17 (1) lit. c Act N° 156(I)/2004 of 30/04/2004). **Poland** explicitly exempts providers from contractual liability towards recipients whose data has been blocked due to a claim for injunctive relief against the provider.[74]

[64] Czech Republic, Hungary, Latvia, Malta, Poland, Slovak Republic, Spain.
[65] Section 10 (5) Information Society Services Law published in OJ No. 183 of 17 November 2004.
[66] Hungary: § 10 ECSA; Malta: § 21 Electronic Commerce Act (Chapter 426) of 10 May 2002 (Act No. III of 2001, as amended by Act No. XXVII of 2002).
[67] Act CVIII of 2001 on certain aspects of electronic commerce services and of services related to the Information Society, available in English translation at http://www.hif.hu/?id=dokumentumtar&mid=632&lang=en.
[68] Article 14 Law of the 25/05/2006 on information society services. Law N° X-614.
[69] Article 14 (1) APSEM.
[70] Section 15 Law No. 458 on providing information society services of 5 June 2002.
[71] § 6 (4) Electronic Commerce Act No. 22/2004 JO of 3 December 2003.
[72] Section 18 Act on electronic commerce and other information society services.
[73] Finish Act 458/2002 of 5th June 2002 on the Provision of Information Society Services available at www.finlex.fi/fi/laki/kaannokset/2002/20020458 .
[74] Article 14 (2), (3) APSEM.

2. Qualification as host provider

In some member states doubts have arisen if providers hosting content for third parties could always be considered as host providers in the sense of Art. 14 ECD. Whereas most cases concern auction platforms there are also some which refer to the "classic" form of hosting third party contents. Thus, a French court classified a host provider not as a provider in the sense of Art. 14 ECD rather than an editor in the sense of press law as the provider (Tiscali) offered to its clients templates in order to generate their own web-site and content. Hence, infringement of intellectual property rights was attributed to Tiscali as an "editor" (in contrast to the liability exemptions of Art. 14 ECD).

3. Actual Knowledge and Unawareness of Facts or Circumstances from which the Illegal Activity or Information is Apparent

The notions of "actual knowledge" and "unawareness of facts or circumstances from which the illegal activity or information is apparent" are crucial for the extent of provider liability. In court practice comparable questions of "knowledge" or "awareness" as well as the notion of "manifestly illegal content" have arisen in the context of national law governing injunctions (e. g. in Austria and Germany) where courts have predominantly not applied those liability exemptions provided for in national e-commerce acts.[75]

In this context the following aspects appear to be most important:

- The preconditions of knowledge or awareness (e.g. positive knowledge or negligent ignorance) and the notion of manifestly illegal content, especially as regards the different types of possibly unlawful information (e.g. copyright or trademark infringements and defamation).
- The formal requirements for notifications of illicit content, in particular the need for an official communication (e.g. in the context of a notice and take-down procedure).

The abovementioned aspects are closely interconnected since a provider must assess the validity of a notice, and verify the identity of the claimant and establish whether or not the claim itself is justified and well-founded (a situation which is particularly difficult where a notice relates to a complex area of law such as copyright). In particular, the notion of "manifestly illegal content" is decisive in determining the extent of the liability to which intermediaries are exposed, since they often do not have the resources necessary to assess the illegality of hosted content. Stakeholders emphasized that there is a risk of pressuring host providers (as well as other types of intermediaries) into the role of an **"**illegitimate judge".[76]

a) Required Level of Knowledge or Awareness

The level of knowledge or awareness required by Article 14 ECD has been the subject of court decisions in **Germany**. Some principles can be deduced from these decisions, such as a concentration on actual, positive human knowledge instead of virtual, automated computer-

[75] see Part 1:B.I.1 below.
[76] Yahoo UK and Ireland; eBay Germany.

knowledge.[77] Negligent ignorance and second-degree (conditional) intent (*dolus eventualis*) do not constitute "knowledge" in terms of § 10 TMG.[78] **"**Knowledge" refers to knowledge of *specific* illegal content since the provider is only able to delete or block accurately identifiable content.[79] General awareness of the fact that illicit offers/material has been posted on a server in the past is not deemed to be equivalent to "knowledge" in terms of § 10 TMG.[80] With regard to claims for damages, host providers enjoy the liability privilege of § 10 TMG only if they are not aware of facts or circumstances from which the illegal activity or information would be apparent (interpreted in German legal literature as absence of gross negligence). Gross negligence can only be assumed in cases of "obvious" infringements.[81]

Similarly the **Netherlands** has implemented Article 14 ECD in such a way that host providers would not be liable if it did not know of the illegal nature of an activity or information, or could not reasonably be expected to know. This second exclusion from liability implies some kind of gross negligence like in Germany.

b) Manifestly Illegal Content

Since actual knowledge or awareness cover not only the actual information or content, but also its unlawfulness, the conditions under which a host provider can be assumed to know or be aware of the unlawfulness of indicated content is crucial. There is a common trend across member states towards a concept of knowledge or awareness being deemed to exist in cases of *manifestly* or *obviously unlawful* content, although this remains a highly controversial issue. As already noted, stakeholders complain about being pressured into the role of an "illegitimate judge" since they are supposed to assess the unlawfulness of content – sometimes on the basis of a vague private notice – in order to decide whether the information should be removed or access disabled. It is however still unclear to what extent providers can be expected to realize the unlawfulness of third-party information. In detail:

The **Austrian** parliament has stated that in its implementation act (ECG) the notion of "actual knowledge" has to be construed restrictively.[82] Austrian courts seem not yet to have decided on the notion of actual knowledge with regard to the interpretation of § 16 ECG. However, the parliament has adopted a doctrine developed by the Supreme Court of Justice, in cases concerning liability of mere contributors, to assist in the interpretation of "actual knowledge" in § 16 ECG.[83] The doctrine – which was also applied in cases regarding injunctions against intermediaries – requires that a person, in order to be liable as a contributor, must deliberately

[77] BGH, 23.9.2003, VI ZR 335/02, NJW 2003, 3764; OLG Brandenburg, 16.12.2003, 6 U 161/02, MMR 2004, 330 (331); OLG Düsseldorf, 26.2.2004, I-20 U 204/02, MMR 2004, 315 (316); LG Düsseldorf, 29.10.2002, 4a O 464/01, MMR 2003, 120 (124).
[78] BGH, 23.9.2003, VI ZR 335/02, NJW 2003, 3764; OLG Brandenburg, 16.12.2003, 6 U 161/02, MMR 2004, 330 (331); OLG Düsseldorf, 26.2.2004, I-20 U 204/02, MMR 2004, 315 (316); LG Düsseldorf, 29.10.2002, 4a O 464/01, MMR 2003, 120 (124).
[79] BGH, 23.9.2003, VI ZR 335/02, NJW 2003, 3764.
[80] LG Düsseldorf, 29.10.2002, 4a O 464/01, MMR 2003, 120 (126).
[81] *Härting*, CR 2001, 271 (276); *Spindler*, CR 2001, 325 (332 f.); *Eck/Ruess*, MMR 2003, 363 (364); *Spindler*, in: Spindler/Wiebe, Internet-Aktionen und Elektronische Marktplätze, 2nd ed. 2004, Kap. 6 Rn. 25.
[82] 817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP, zu § 16.
[83] 817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP, zu § 16.

promote the direct infringer's actions - which could only be demonstrated where an infringement was "obvious to any non-lawyer without further investigation".[84] The legislator transferred these criteria to the interpretation of "actual knowledge" in terms of § 16 ECG[85], stating that an "infringement obvious to a non-lawyer without further investigations" was in other words an infringement whose unlawfulness is "easily noticeable" for the intermediary in the same way as for any other person. Actual knowledge is only established in cases where the intermediary is certain about the unlawful nature of the conduct or information.

In **Austria** there have been a number of court decisions dealing with injunctions related to the question of manifestly illegal content or infringements "obvious to a non-lawyer without further investigation". Obvious infringements were found by Austrian courts for example, in the case of the unauthorized registration of the generally known name of an Austrian political party as a domain ("fpo.at").[86] In another case concerning competition law the Supreme Court of Justice held that legal considerations referring to advertising and general terms and conditions far exceeded what is identifiable to a non-lawyer as being obviously illegal without further investigation.[87] Another court dealing with trademark infringements and defamation held that infringements of trademark law could not be qualified as being obvious to a non-lawyer, but decided that insulting statements and defamation of business reputation was capable to being determined by everybody.[88] Trademark infringements by linking keywords (adwords) to advertisements have also been held not to be obvious normally.[89]

German courts have not had to decide on the preconditions of obvious unlawfulness, but comparable questions arise in context of injunctions. Based on the legal doctrine of "accessory liability"[90] an injunction may be issued under the condition that the provider had knowledge of a "clear infringement"[91] and nevertheless failed to prevent further infringements of this kind. The courts have not yet reached a common consensus on the criteria to assess a clear infringement, though the Federal Court of Justice has approved them in cases of trademark infringement (committed through the sale of faked ROLEX watches on auction platforms).[92]

French courts have not had many opportunities to clarify the notion of "illicit" content. However, the Conseil Constitutionnel stated the "illicit" has to be interpreted as "manifestly

[84] AU6. – OGH, 6/7/2004, 4 Ob 66/04s; AU12. – OGH, 13/9/2000, 4 Ob 166/00s; AU13. – OGH, 12/9/2001, 4 Ob 176/01p; AU7. – OGH, 24/5/2005, 4 Ob 78/05g; AU9. - OGH, 19/12/2005, 4 Ob 194/05s; AU8. - OLG Innsbruck, 24/5/2005, 2 R 114/05i, dietiwag.org II.
[85] 817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP, zu § 16.
[86] AU12. – OGH, 13/9/2000, 4 Ob 166/00s, http://www.internet4jurists.at/entscheidungen/ogh4_166_00s.htm; AU13. – OGH, 12/9/2001, 4 Ob 176/01p, http://www.internet4jurists.at/entscheidungen/ogh4_176_01p.htm.
[87] AU6. – OGH, 6/7/2004, 4 Ob 66/04s, http://www.internet4jurists.at/entscheidungen/ogh4_66_04s.htm.
[88] AU8. - OLG Innsbruck, 24/5/2005, 2 R 114/05i, http://www.internet4jurists.at/entscheidungen/olgi_114_05i.htm
[89] AU9. - OGH, 19/12/2005, 4 Ob 194/05s, http://www.internet4jurists.at/entscheidungen/ogh4_194_05s.htm.
[90] See in extenso Country Report Germany Part 1, A. I..
[91] See for example GE 12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I; GE13. – BGH, 19.4.2007, I ZR 35/04, MMR 2007, 507 - Internetversteigerung II; GE15. - OLG München, 21.9.2006, 29 U 2119/06, MMR 2006, 739.
[92] GE 12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I; GE13. – BGH, 19.4.2007, I ZR 35/04, MMR 2007, 507 - Internetversteigerung II.

illicit" (in the light of Art. 14 ECD). Yet, the court did not specify more this notion.[93] We note only some cases in which the courts referred explicitly to "manifestly illicit" content, sometimes mixed up with the issue of manifest troubles which are the basis for preliminary injunctions against providers (according to civil procedure code). Hence, one court held that the sale of copyrighted video games well below under the counter price constitute such a "manifest" infringement (and granted an injunction based on civil procedure).[94] In another case, the TGI Paris declared that the violations of privacy (atteinte a la vie privée) can not be deemed as being "manifestly illicit".[95] The Court of Appeal, Paris,[96] qualified as "manifestly illicit" all racist[97], anti-Semitic[98] or revisionistic contents[99] as well as texts which excuse crimes of war, paedophilia[100] or pornographic pictures and contents.[101]

In **Belgium** the "exposé des motifs" of the LSSI states that content has to be obviously illicit regarding the "illegal" nature of the activity or information actually known, which for example applies in cases of child pornography, revisionism or incontestable defamation. Courts seem to accept an expansive interpretation of the notion of knowledge or awareness. The Belgian Supreme Court[102] considers that the domain owner and operator of a website containing hyperlinks referring to child pornography has control and knowledge of these illegal hyperlinks even if it did not insert them (but the hyperlinks were proposed by others on its website). Consequently, the judge refused to accord the host provider's liability exemption to the website titular.

With regard to the credibility of a notification the **Dutch** legislature has stated that a "simple notification" could be adequate to result in "actual knowledge" on the part of the intermediary

[93]Conseil Constitutionnel Décision n° 2004-496 DC - 10 juin 2004. http://www.conseil-constitutionnel.fr/decision/2004/2004496/index.htm

[94] FR13 – Comm Paris, 17/10/2006, Konami c/ Babelstore www.droit-technologie.org/jurisprudence/details.asp?id=224.

[95] FR43. – TGI Paris, 19/10/2006, Mme H.P. c/ Google France, http://www.juriscom.net/documents/tgiparis20061019.pdf.

[96] FR44. – CA Paris, 08/11/2006, Comité de défense de la cause arménienne c/ M. Aydin S., SA France Télécom services de communication résidentiels, http://www.foruminternet.org/telechargement/documents/ca-par20061108.pdf.

[97] TGI Paris, ord. ref., 12 juillet 2001 http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord_tgi_paris_120701.htm

[98] TGI Nanterre, 24 mai 2000 http://www.juriscom.net/txt/jurisfr/cti/tginanterre20000524.htm, FR34. – TGI Paris, 20/11/2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf; FR33. – TGI Paris, 22/05/2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France, http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm#texte.

[99] FR2. – TGI Paris, 13/06/2005, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1139 http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf. Confirmé par Paris 11ème ch., 24 nov. 2006.

[100] Recommandation Les enfants du Net II : Pédo-pornographie et pédophilie sur l'Internet, 25 janvier 2005, http://www.forumInternet.org/recommandations/lire.phtml?id=844,

[101] FR23. – TGI Paris, 27/02/2006, Alain Afflelou / Google, Free, http://www.legalis.net/breves-article.php3?id_article=1648, http://www.legalis.net/jurisprudence-decision.php3?id_article=1648.

[102] BE20. – Cour de cassation, 3.2.2004, *R.D.T.I.*, 2004, n° 19, n° P.03.1427.N, (V.R. c. ministère public).; En première et seconde instance : BE18. – Tribunal de première instance d'Hasselt (correctionnel), 1.3.2002, *Inédit*, (ministère public c. V.R.) ; BE19. – Cour d'appel d'Anvers, 7.10.2003, n° 440 P 2002, *A.M.*, 2004, liv. 2, pp. 166 et s., (V.R. c. ministère public).

where, within reason, it is impossible to doubt the accuracy of the notification which is definitely the case, if the content/information being complained about is "unmistakably" illegal. In the case of *Lycos vs Pessers*[103], the Supreme Court of the Netherlands held that certain defamatory content was not unmistakably unlawful and the host provider consequently could not be held liable.

The situation in **Portugal** is somewhat similar. Host providers (and also hyperlink and search engines providers) are only (criminally) liable if they are aware of an obviously illegal activity and take no action.[104] A more expansive approach applies to civil liability where a provider is civilly liable if it is or should be aware of the illegal nature of the information.

Under **Swedish** law, once a host provider has been found to have actual knowledge of the illegal nature of material (here: incitement to hatred of sexual minorities) on a website without removing it, it may be found guilty as an accomplice of complicity in crime. In the "online guestbook" case the operator was found guilty of complicity in incitement to hatred of sexual minorities. The court found that by failing to remove and by commenting on the message he was aiding and abetting the crime of the user.[105] Just recently the Swedish Supreme Court decided that an operator of a bulletin board under general criminal law did not have any obligation to delete a user's illegal message. Since it had not been "obvious" that the message was illegal the operator had no obligation to do so under the Act on the Responsibility for Bulletin Boards.[106]

Czech and **Slovak** law uses the concept of conscious negligence (*culpa lata*) as the basis for legal responsibility on the part of host providers. First, it must be proven that the host provider had obtained knowledge of the illegal nature of the information provided by the user. Second, the fact that the provider is aware of the information as such does not directly imply its awareness of its illegal nature. Its knowledge of the illegality depends largely on the nature of the illicit information, e.g. child pornography (where a judgement can be easily made) or copyright infringements (where it is hard to tell). The assessment of the information of which the provider is aware of is based on the following principles: a) if the information violates public (imperative, absolute) laws such as criminal law, the provider is obliged to reveal its illegality proactively; and b) if the information infringes individual private (relative) rights, the intermediary is not to be expected to reveal this proactively.

The distinction based on the types of infringements in question is reflected in the different formal requirements for notices issued against intermediaries under **Finnish** law in cases of serious and less serious offences (see c)bb) below). Only when a communication is dealing with obviously serious offences like child pornography is an "informal" notification sufficient for the intermediary to have obtained knowledge. By contrast, notifications on less serious

[103] NE11. – District Court of Haarlem, 11/09/2003, *Lycos Netherlands BV vs Mr Pessers***,** LJN number AL1882, case number 94609/KG ZA 03-426, disponible via www.rechtspraak.nl; NE12. – Appeals Court of Amsterdam, 24/06/2004, Lycos Netherlands BV vs Mr Pessers; NE13. – Supreme Court, 25/11/2005, Lycos Netherlands BV vs Mr Pessers, LJN number AU4019, case number C04/234HR, available via www.rechtspraak.n

[104] Articles 16-18 of the Portugues Transposition Act

[105] SW1 - Hovrätten för Västra Sverige 18.5.2006 -B 2588-05.

[106] The ruling is not yet available in writing.

matters such as copyright infringements have to meet the formal requirements of section 22 of the Finnish implementation act.[107] For all other issues it takes a court order to oblige the provider to disable access to the notified content.

Summing up content can be regarded as manifestly illegal where it includes clear-cut criminal activities like child pornography which are noticeable for any non-lawyer. Manifest unlawfulness is even more problematic where intricate questions of, trademark, copyright or competition law have to be dealt with, which often cannot be answered without professional legal advice. In such cases much will depend on the credibility and authority of the person or entity who has given a notification of unlawful content to the intermediary.

c) Formal Requirement for Notifications

Very different requirements for notifications to intermediaries can be found amongst EU member states. Whilst some legal systems do not explicitly regulate any requirements for notifications – so that a mere private letter can sufficiently establish knowledge of an infringement – other member states stipulate a number of formal requirements, sometimes linked to a statutory notice and take-down procedure. Requirements for notifications are particularly important for establishing the preconditions of knowledge or awareness for intermediates' liabilities. The content of communications – details of the nature of the infringement and proof of the infringed right, for example – can determine whether the intermediary has obtained knowledge of content and – even more importantly – of its unlawfulness. Moreover, the addressee of notifications within a company is crucial for the internal information flow and consequently the intermediary's ability to terminate and prevent infringements. In practice, right holders frequently submit notices in a variety of forms and to individuals who do not have specific responsibility for dealing with such complaints. Much depends on the credibility of the person or entity giving the notice. The problem of assessing the unlawfulness of notified content and the credibility of notices is however particularly problematic since the ECD puts an intermediary in a position where it has to act "expeditiously" as soon as it is put on notice regardless of whether it is sure about the legality of the content in question.

aa) Member States without Formal Requirements

In a number of member states, especially those who do not provide for a notice and take-down procedure, no formal requirements for notification of unlawful content have been established.

Dutch law does not provide for formal requirements for notifications. The parliamentary papers[108] dealing with the concept of actual knowledge state however that a "simple" notification – such as a message given by any person - is not sufficient, whereas a court order is always considered to constitute actual knowledge. The exact extent of this notion, however,

[107] The notice-and-take-down procedure of Finland, more details see below Part 1:A.I.
[108] Parliamentary documents of the Dutch Lower House 2001/02, 28 197, N°3, p. 49. Can be found using www.overheid.nl/op .

still remains unclear, in particular as regards the preconditions to describe a notification as not "simple".

In **Germany** a notice may in principle be given by any person or authority. However, courts have nonetheless demanded certain minimum standards for notifications. In a case dealing with copyright infringements committed on an auction platform, the operator of the auction platform did not obtain notice of a clear copyright infringement when the plaintiff initially objected to the distribution of certain text passages, since that notice did not contain details on the claimed copyright. Not until a second notification, this time including copies of the text passages offered on the auction platform as well as confirmation of the plaintiff's copyright, was the intermediary put on notice.[109] In **German** legal practice (in particular as regards copyright and competition law) a so-called warning[110] combined with the requirement of a declaration by the provider to cease and desist (i.e. to block the access to the illicit content and/or to remove it) is used to make the provider aware of the fact that illicit content is hosted or illicit activities are ongoing. Thus, following a warning the provider can not claim that it has no knowledge of the content or activity. Furthermore, the provider has to bear the costs of the warning (i.e. of the lawyer who has drawn up the warning) as courts qualify the lawyer as an agent of necessity who acts in the interests of the provider.

Few cases have dealt with question of attributing knowledge of third persons, such as employees, to a provider. In an **Austrian** case, knowledge of unpaid moderators of an online forum was not attributed to the provider, since these persons were unknown to the provider and the court consequently deemed the relationship between them as lacking sufficient proximity to justify an attribution of knowledge.[111] In the case of *Godfrey v. Demon* a **British** intermediary was still legally "on notice" although notice had been given by sending a letter by "fax" to its managing director who had no specific responsibility for such complaints.

bb) Member States Providing for Formal Requirements

Other member states acknowledge specific notifications by an authority.[112] Article 16.1 (b) of the **Spanish** e-commerce law establishes that the service provider shall be understood to be genuinely aware when "a competent body has declared the data to be illegal, has ordered its removal or that access to the data be blocked, or when it has been declared that damage has been done, and the provider is aware of the relevant resolution, without prejudice to the notice and take down procedures that apply to the providers on the basis of voluntary agreements and of other effective knowledge-based means that can be established". The "competent body" can be a court or an administrative authority, which acts in the exercise of its legal competences (according to Spanish authors and stakeholders). Consequently, some intermediaries refuse to take appropriate measures when rights holders notify them an illicit content.

[109] GE15. - OLG München, 21/9/2006, 29 U 2119/06, MMR 2006, 739.
[110] For an explanation of the term „warning" see the Country Report Germany Part 1 A. III..
[111] AU4. – OLG Wien, 3/8/2006, 3 R 10/06x, http://www.internet4jurists.at/entscheidungen/olgw_10_06x.htm.
[112] Note that the issue disputed among stakeholders (like in Italy) if these implementations comply with Article 14 ECD will not be addressed in this section.

Furthermore, "actual knowledge" required for criminal and civil liability is interpreted restrictively. According to the Provincial Tribunal of Madrid[113] even a notarized notification is not sufficient to establish "actual knowledge" - the Examining Magistrate of Barcelona[114] followed that interpretation and denied actual knowledge on the part of a provider of hyperlinks (who is subject to the same liability rules like host providers) even though it had known that the links were leading to contents conflicting with competition law. On the contrary, the judge of the "Audiencia Provincial de Cáceres"[115] seemed (but the decision is unclear and not final) to follow an "open interpretation" of the notion as it admitted other ways of obtaining "actual knowledge" (like factual elements).

This conflict culminates in the famous case *SGAE (General Society of Authors and Editors) v. "Asociación de Internautas" (Internet Users Association) case* where the trial judge[116] held the intermediary liable for defamatory contents hosted on its (mirror) website. From the perspective of the judge, the intermediary had the **obligation to monitor** this content. Surprisingly, the host provider's legal exemption was not referred to. The appeal decision[117] confirmed the host provider's liability. The judge refused to allow for the liability exemption because the intermediary had "effective knowledge". No "competent body" (Article 16.1 (b) of the e-commerce Spanish law) had previously ordered the removal of illegal information. In consequence, we can infer that the judge had applied an expansive interpretation of "actual knowledge" (contrary to the common understanding). The case has been brought before the Supreme Court[118] where the "Asociación de Internautas" pleaded for the submission of a preliminary reference to the European Court of Justice. The "Asociación de Internautas" wishes to obtain clarifications on the ECD intermediaries' liability provisions (and particularly those dealing with the hosting activity and the notion of "actual knowledge"). The Supreme Court decision on whether to grant a preliminary reference is not known at the present time.

Similar discussions are reported in **Italy.** Article 14 of Legislative Decree No. 70 states: "does not have actual knowledge of the fact that the activity or information is illegal and, as regards claims for damages, is not aware of facts or circumstances that make it apparent that the activity or information is illegal". According to legal scholars,[119] the actual knowledge standard is to be applied exclusively in criminal cases, whilst the awareness test is sufficient in cases involving damages claims. Aside from the fact that there seems to be no prevailing opinion amongst legal scholars concerning the interpretation of actual knowledge of

[113] SP5 - Appeal decision n° 835/2005, of the Provincial Court of Madrid (section n°14), 20.12.2005, (don Mauricio v. *I Espana Reseaux SL*), appeal request n° 229/2005.
[114] SP9 - Decision (*Auto*) of the Examining Magistrate (Barcelona), March 7th, 2003, DP 872/02-C.
[115] SP4 - Provincial Court of Cáceres (*Auto*) (section n° 2), October 30th, complaint n° 353/2006.
[116] SP6 - Decision (Sentencia) n° 00126/2005, Court of first instance of Madrid, 15.06.05 – Litigation SGAE (Sociedad General de Autores y Editores v. *Asociación de Internautas)*.
[117] SP7. - Decision of the Provincial Court of Madrid, 06.02.06, request n° 841/2005 – Litigation SGAE (*Sociedad General de Autores y Editores* v. *Asociación de Internautas*).
[118] Supreme Court, procedure n° 0000914/2006.
[119] Giovanni M. Riccio, *La responsabilità civile degli internet providers*, Torino, Giappichelli, 2002; Francesco Di Ciommo, *Evoluzione tecnologica e regole di responsabilità civile*, Napoli, ESI, 2003

apparently illegal contents or activities, Article 14 ECD has been implemented into Italian law by Article 16 Legislative Decree No. 70. In contrast to other member states, Article 16 requires providers to act expeditiously (to remove or to disable access to the information) *only* upon notice from the relevant authorities. Whereas copyright holders complain about this restriction, intermediaries are obviously uncomfortable as to whether they should inform their users about receipt of notifications of illicit contents, since this could make them liable for complicity or aiding and abetting under Article 378 of the Italian Criminal Code. This Article punishes a person who, after a crime has been committed, helps the offender to evade the investigation or arrest by the authorities – a doctrine that is interpreted by Italian courts widely so as to include acts or omissions,[120] and which can be applied to acts either before or after investigations have been started.[121] In one case a Court in Catania[122] applied Article 16 of Legislative Decree No. 70 in stating that host **providers do not have any duty or obligation to monitor** their networks for illegal activity, or to disable or block customer access to websites not under the service provider's direct control or on its network. The court held that hosting providers can be held liable for negligent behaviour, in cases where they are aware of the presence on the website of potentially illegal material and do not act expeditiously to ascertain the actual illegality of such material and remove it. Additionally, a hosting provider can be held liable for fraud or malice where it is aware of the presence of such material and does not act to remove it.

The **Portuguese** implementation act[123], Article 18, imposes an important restriction on "private" notifications: "In the cases considered in Articles 16 and 17, the intermediary service provider, if the illegality is not revealed, shall not be obliged to remove the disputed content or disable access to the information only because of the fact that a third party is arguing an infringement".

The approach taken by **Finland** is more complex. Section 15 of the national implementing legislation stipulates that a provider shall not be liable if it removes the illicit content:

- upon obtaining knowledge of the order concerning it (from a court) or if it concerns a violation of copyright or similar rights upon obtaining the notification referred in section 22 (notice and take-down procedure)
- upon otherwise obtaining actual knowledge of the fact that the stored information is clearly contrary to Section 18 of chapter 17 of the Section 8 of Chapter 11 of the Penal Code (Incitement hatred against an ethnic group, pornographic images showing children, violence, bestiality).

Hence, Finnish law distinguishes between three cases that trigger the liability of a host provider, when it ignores: (i) an order issued by a court (ii) a notification of a copyright infringement according to the notice and take-down procedure, or (iii) for certain criminal offences, the notification of content that "clearly" constitutes a "serious" offence. The aim of Finnish law seems to be to distinguish between different degrees of awareness concerning

[120]Cf. Court of Cassation, November 3, 1997, Lenza
[121]Court of Cassation, June 21, 1990, Tarlindano
[122]June 29, 2004, http://www.ictlex.net/index.php/2004/06/25/tribunale-di-catania-sez-iv-civile-sent-228604
[123] Law- Decree No. 7/2004 of 7 January 2004 (Diário da republica I-A n° 5 de 7/1/2004 p. 70)

illicit content. Whereas it might be quite difficult for a provider to assess correctly the legal implications of a copyright or trademark, there should not be much doubt about the illegality of paedophilia.

Another approach that gives leeway for courts in general, but at the same time establishes some guidelines for interpretation, is the way the **UK** has implemented Article 14 ECD: Whereas the British implementation Regulation 19 of the Electronic Commerce (EC Directive) Regulations 2002[124] follows verbatim the wording of Article 14 ECD, the UK provides in Regulation 22 specific criteria to determine whether a service provider has actual knowledge (see Regulations 18(b)(v) (caching) and 19(a)(i) (hosting) of the E-Commerce Regulations). Courts should thus take into account all matters which appear to it in the particular circumstances to be relevant, in particular whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c), and the extent to which any notice includes the full name and address of the sender of the notice, details of the location of the information in question and details of the unlawful nature of the activity or information in question. Following the criteria set out in Regulation 22, the High Court (Queen`s Bench Division) rejected liability on the part of British Telecom as a host provider following receipt of a notice which did not contain the location of a defamation allegation nor details of the unlawful nature of the activity or information.[125]

Moreover, the Home Office has issued guidelines[126] to law enforcement authorities on how to issue notices to hosting providers for content which breaches regulations under the Terrorism Act 2006.[127] These stipulate that content must be assessed, and notices issued, by a single designated law enforcement agency (in this case, the anti-terrorism branch of the Metropolitan Police), in a specified form and served on the personnel at the hosting provider's address who have responsibility for such matters.

Finally, **France** has opted for an optional notification procedure: The LCEN (art. 6-I-5 LCEN) has introduced a non-mandatory procedure concerning the necessary elements of a notification, however, without any counter-notice. It could be used for any kind of illicit contents but is restricted to host providers. The French procedure can not exactly be compared to a Notice-and-take-down-procedure like it is practiced in Finland or the US as it doesn't imply a take down automatically after the notification; the obligation to remove the content, however, results from the LCEN directly if the provider has been notified. Moreover, the French procedure does not prejudice liability questions.

If this procedure is followed meticulously, actual knowledge of the provider is presumed by the LCEN. Art. 6-I-5 LCEN as follows:

[124] Statutory Instrument 2002/2013, available at: http://www.opsi.gov.uk/si/si2002/20022013.htm.
[125] UK2. - Queen's Bench Division 10.3.2006- [2006] EWHC 407 (QB); [2006] 3 All ER 336; [2006] EMLR 523- Bunt v Tilley & Others
[126] Available at: http://security.homeoffice.gov.uk/news-publications/publication-search/legislation-publications/guidance-notices-section3-t.pdf?view=Binary.
[127] See Part 1:B.III.2.b) and Part 1:A below

> "The persons cited in subparagraph 2 shall be deemed as being aware of the disputed facts when the following information is notified to them:
>
> - The date of the notification;
>
> - If the notifying person is a natural person: their surname, forename, profession, residence, nationality, date and place of birth; if the applicant is a legal entity: its form, name, registered office and it legal representative
>
> - The name and residence of the recipient or, if this is a legal entity, its name and registered office;
>
> - A description of the disputed facts and their exact location;
>
> - The reasons for which the content must be removed, including an indication of the legal provisions and justification of the facts;
>
> - a copy of the correspondence addressed to the author or producer of the disputed information or activities requesting them to be stopped, removed or amended, or proof that the author or producer could not be contacted."

This procedure of notification described in art. 6.I-5 LCEN has to be followed meticulously and strictly. If not, the person in charge must be stated as non liable.[128]

The French Government has installed several websites which detail illicit web-sites and dangers of the Internet and where people can report illicit contents they have discovered.[129]

d) Onus of Proof

In **German** law the onus of proof is, in general, laid on the plaintiff and this is also the case concerning the actual knowledge of the provider.[130] It is up to the plaintiff to prove that all elements of the liability exemption are not applicable in the specific case. The same rule applies in **Belgium**. In the UK, the DTI Guide for Business to the Electronic Commerce states that the onus will be on the enforcement authorities or the plaintiff to demonstrate that a service provider had actual knowledge but did not act appropriately upon obtaining it,[131] however the **British** enforcement authorities are expected to place the onus on the service provider to demonstrate that it has complied with the requirement of expeditious removal.[132]

Furthermore, the **UK** has introduced with Regulation 21 – which is not an implementation of the E-Commerce Directive – a provision that is not found in other Member States: this applies where a service provider charged with an offence in criminal proceedings arising out of any transmission, provision of access or storage falling within Regulation 19 (but also Regulations

[128] FR44. – CA Paris, 08/11/2006, Comité de défense de la cause arménienne c/ M. Aydin S., SA France Télécom services de communication résidentiels, http://www.foruminternet.org/telechargement/documents/ca-par20061108.pdf

[129] By example: www.Internet-mineurs.gouv.fr/)

[130] BGH, 23.9.2003, VI ZR 335/02, NJW 2003, 3764 concerning § 5 TDG (old version); OLG Düsseldorf, MMR 2004, 315 (317) concerning § 11 TDG; *Spindler*, in : Spindler/Schmitz/Geis, § 11 TDG Rn. 65.

[131] DTI, Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013)" p. 26 s., http://www.dti.gov.uk/files/file14635.pdf.

[132] DTI, Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013)" p. 26, http://www.dti.gov.uk/files/file14635.pdf.

17 and 18 concerning mere conduit and caching), relies on a defence under the Regulations. It provides that, where evidence is adduced which is sufficient to raise an issue with respect to that defense, the court or jury must assume that the defence is satisfied unless the prosecution provides beyond reasonable doubt that it is not. However, there is no case law on this issue.

4. Relationship to Press Law

In the early days of internet law, discussion arose on analogies to Press law on the grounds that host providers could technically be viewed as "publishers" helping to distribute and disseminate third party content. Thus, the High Court (Queen's Bench Division)[133] decided that an internet provider hosting newsgroups with defamatory content had to remove it after notification thereof (treating the provider as a publisher). However, today - as far as has been reported - Member States do not generally treat host providers as press publishers, notwithstanding reservations in some specific cases such as those involving operators of discussion forums closely linked to online press publications.[134] Some courts have explicitly affirmed this perspective; for example the **French** court TGI of Paris [135] has stated that French legislation on the Press is not applicable. However, the same court stated that concerning MySpace as a typical Web 2.0 application press law is prevailing over liability exemptions of the LCEN (French law implementing the ECD),[136] similar to a previous case[137] regarding "Second Life".

Similarly, a **Spanish** judge[138] explicitly refused to compare the situation of a publisher with the situation of a host provider. However, courts in other Member States, such as **Poland**, still apply Press Law, in particular to host providers of online discussion forums. Thus, a Polish trial court[139] held that a host provider (deemed in the eyes of the court to be the "publisher" of an online discussion forum, i.e. the operator) had to control the comments in the forum before "publication" – which has been widely criticised as not conforming to Article 14 APSEM.

In an **Italian** case the court of Catania affirmed that press law can not be applied to ISPs (especially articles regulating publisher liability), nor can vicarious liability rules. By this statement, this decision has overruled some precedents held by Italian courts before the implementation of ECD.[140]

---

[133] UK3 - High Court, Queen's Bench Division (Handed Down at Leicester Crown Court) 26.3.1999 Case No: 1998-G-No 30, [1999] E.M.L.R. 542 - Godfrey v. Demon Internet Limited.
[134] Cf. the cases in Germany concerning internet discussion forums GE5 - BGH, 27.3.2007, VI ZR 101/06; OLG Hamburg, 22.8.2006, 7 U 50/06, MMR 2006, 744 – heise.de.
[135] FR7. – TGI Paris, 16/02/2005, Dargaud Lombard, Lucky Comics/Tiscali Média, http://www.legalis.net/breves-article.php3?id_article=1420.
[136] FR 46. – TGI Paris Lafesse / MySpace, TGI Paris, Référé 22/06/2007, *Jean Yves L. dit Lafesse / Myspace* http://www.legalis.net/breves-article.php3?id_article=1965
[137] FR47. – TGI Paris, référé 02 juillet 2007, Associations Union départementale des associations familiales de l'Ardèche et Fédération des Familles de France c/ Linden Research Inc, SAS Free, SA Neuf Cegetel et autres, http://www.legalis.net/jurisprudence-decision.php3?id_article=1960 .
http://www.droit-technologie.org/upload/jurisprudence/doc/230-1.pdf.
[138] SP5 - Provincial Court of Madrid, appeal decision n° 835/2005, (section n°14), 20.12.2005, (don Mauricio v. I *Espana Reseaux SL*), appeal request n° 229/2005.
[139] PO1 - Sąd Rejonowy w Słupsku 7.3.2007.
[140] IT3 - Court of Catania, June 29, 2004.

B. Obligations to Block or Remove Illicit Content and Prevent Future Infringements (Injunctions)

As already stated most of the court cases have concerned injunctions. Whereas most of the cases can be allocated to a specific service covered by the ECD there are nevertheless some common features and issues which should be discussed in general terms since they apply irrespective of the type of intermediary or content in question. We differ then between injunctions against specific types of providers (access/mere conduit and host providers) as well as between injunctions issued by civil courts and public authorities. Last but not least the technical measures ordered by courts or authorities will be described.

I. General Issues

1. Applicability of Liability Exemptions

The majority of Member States explicitly implemented the exceptions to articles 12 (3), 13 (2), and 14 (3) ECD concerning the power of a court or administrative authority, in accordance with Member States' legal systems, to require the service provider to terminate or prevent an infringement.[141] The **French** article 6-I-8 LCEN however excludes caching providers and consequently incorporates only articles 12 (3) and 14 (3) ECD, but not article 13 (2) ECD. A second group of Member States did not incorporate articles 12 (3), 13 (2), 14 (3) ECD into their national legislation.[142] which nevertheless does not appear to stop their courts and authorities issuing injunctions and administrative orders for the termination or prevention of infringements.

In Member States with case law dealing with injunctions against intermediaries the national provisions corresponding to articles 12 (3), 13 (2), and 14 (3) ECD were construed in such a way as to exclude injunctions and other judicial or administrative orders to terminate or prevent infringements. The liability exemptions have been thus restricted to civil liability for damages or criminal responsibility.

This applies to the **Austrian** Supreme Court, which ruled that the liability exemption of § 16 ECG (regarding host providers) only exempts a defendant from possible liability for damages and criminal prosecution, but leaves untouched claims for injunctive relief under civil law.[143]

Likewise in the **British** case Bunt v Tilley the court referring to Regulation 20 (b) found the E-Commerce Regulations would not preclude an injunction, but only apply to financial and criminal sanctions.[144]

The **German** Federal Court of Justice ruled – particularly referring to § 7 (2) 2nd Sentence TMG (incorporating articles 12 (3), 13 (2), and 14 (3) ECD) – that the liability exemptions of

[141] Austria, Cyprus, Finland, Germany, Greece, Hungary, Ireland, Italy, Lithuania, The Netherlands, Slovak Republic, Spain, United Kingdom.
[142] Belgium, Denmark, Czech Republic, Estonia, Latvia, Luxembourg, Malta, Poland, Portugal, Solvenia, Sweden.
[143] AU2. – HG Wien, 21/6/2006, 18 Cg 67/05, http://www.internet4jurists.at/entscheidungen/hg67_05w.pdf.
[144] UK1. – Queen's Bench Division, 10/3/2006, [2006] EWHC 407 (QB); [2006] 3 All ER 336; [2006] EMLR 523, Bunt v Tilley & Others

the TMG are not applicable to injunctions based on claims for termination of or refraining from infringements. [145] In a recent decision the Federal Court of Justice in addition referred to Recital 48 whereupon the ECD does not affect the power of Member States to require service providers who host information provided by recipients of their service to apply those duties of care that can reasonably be expected from them and which are specified by national law, to detect and prevent certain types of illegal activities.[146]

In the "Bitmailer" case a **Spanish** judge decided[147] (in a case regarding copyright infringements) that the liability exemption provided for by Article 14 of the LSSICE (mere conduit activity) excluded preliminary and preventive injunctions of cessation (as provided by Spanish e-commerce law and copyrights law) against a mere conduit provider who benefitted from the liability exemption. From the judge's point of view an injunction could only be based on Article 11 LSSICE, which states that "When a body competent in the field has ordered, in the exercise of the duties legally conferred on them, that the provision of an information society service be stopped or that certain content from providers established in Spain be taken down, and the cooperation of the intermediary services providers is necessary to this, it shall be able to order these providers [...] to suspend transmission, data storage, access to the telecommunications networks or the provision of any other equivalent intermediary service that they undertake". The judge in the Bitmailer case found however that he was not competent to order an injunction on the basis of this provision.

It should be noted that the decision has been handed down before the Enforcement Directive has been implemented in Spain (which now clearly provides for an injunction against providers); moreover, this decision has been criticized by most Spanish scholars and is unlikely to be followed by other courts. In sum, the "Bitmailer"-decision obviously is highly controversial and can not be taken as a predominant case for Spain.

2. Subsidiarity

It is in addition a matter of dispute between Member States whether there is any kind of subsidiarity principle that could be applied to injunctions against providers. Such a principle would require that in the first instance the content provider (tortfeasor, infringer) has to be sued; only if this claim fails can an injunction against a host or access provider be filed. This principle may be extended in such a way to allow a host provider (after the content provider) has to be sued; only a the last resort might an injunction against the access provider be applied for.

French Courts for example have used such a principle pursuant to Art. 6-I-8 LCEN in handing down injunctions against *access providers* only if *host providers* failed to act or

[145] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I ; GE13. – BGH, 19.4.2007, I ZR 35/04, MMR 2007, 507 - Internetversteigerung II; see also GE14. – BGH, 12.7.2007, I ZR 18/04.

[146] GE14. – BGH, 12.7.2007, I ZR 18/04

[147] Commercial tribunal of Madrid N°2, 10.11.2004, (Emi Music and others v. Bitmailer, webpage weblisten.com), request n° 14/2004.

where actions against such providers proved inneffective. In the Aaargh case[148], it is still disputed whether the judge has first to check whether host providers acted efficiently before ordering injunctions against access providers. Nevertheless the Court of Appeal confirmed that the subsidiarity principle was properly applied. The Supreme Court is due to give a final decision on the case and to specify mechanisms of subsidiarity in the near future, in particular how precise such an injunction has to be in order to be carried out by a host provider. The French courts, however, have not yet had to assess the subsidiarity principle with regard to the relationship between a content provider and *host provider*; in other terms: they had not to decide whether the author/content provider had to be sued first, and the host provider only by default .

Contrary to these French rulings the **German** Federal Court of Justice recently endorsed the principle that there is no subsidiarity regarding injunctions against host providers, citing issues of privacy under the doctrine of "accessory liability" – Störerhaftung.[149] Hence, it is not necessary for a right holder to sue the author of the illicit content in the first place rather than to apply directly for an injunction against the host provider as the contributor to the infringement. However, it has to be noted that this decision concerned host providers rather than access providers – nevertheless, provided an access provider could be deemed an accessory ("Störer"), i.e. a contributor to the infringement, it seems likely that German courts would not apply any principle of subsidiarity. The **German** Interstate Agreement for Broadcasting and Telemedia (Rundfunkstaatsvertrag – RStV[150]) authorises the competent public authorities to issue orders against an access provider where an order against the person directly responsible for the unlawful content is not feasible or not promising (§ 59 (4) RStV). In addition, according to § 59 (5) RStV administrative orders are subsidiary in cases of infringements of private rights where the rightholder has private cause of actions. In such cases an administrative order is only to be issued where required for reasons of common welfare.[151]

3. Injunctions and Art. 15 (1) ECD

A possible conflict between injunctions or administrative orders and Article 15 (1) ECD is a matter of debate in a number of Member States. Injunctions ordering a defendant to refrain from infringements result in a legal situation where intermediaries are effectively obliged to monitor their services in order to prevent breach of the injunction in case of new infringements. Furthermore some Member States have legal systems that make the violation of an obligation to examine a precondition for the issue of an injunction.

[148] FR1, FE2, FR3 - http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf Court d`Appel (CA) Paris, 24 novembre 2006, SA Tiscali (Telecom Italia), AFA, France Telecom et a. c/ UEJF, J'Accuse, SOS Racisme et autres.
[149] GE5. – BGH, 27/3/2007, VI ZR 101/06, MMR 2007, 518, in a case concerning a discussion forum (hosting).
[150] Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV) vom 31.8.1991, zuletzt geändert durch Art. 1 des Neunten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 31.7. bis 10.10.2006 (GBl. BW 2007 S. 111) effective since March 3, 2007.
[151] See Country Report Germany Part. 1 B. II. 2..

As injunctions (or orders to block access etc.) lead de facto to an obligation to monitor activities on websites or the traffic at an access-point, there has been discussion in some Member States about the relationship between injunctions (which are not covered by liability exemptions (Art. 12 (3), 13 (2)and 14 (3) ECD)), and the prohibition of general monitoring obligations (Art. 15 ECD). It has been discussed within courts and in academic circles how obligations to monitor arising from an injunction order ("specific monitoring obligations") can be reconciled with the non-existence of general monitoring obligations:

There is a lively debate on this matter in both Germany and Italy: for example, the **German** Federal Court of Justice ruled that once a provider (in the case in question, an auction platform that had been classified to be a host provider) obtains notice of an infringement, the provider is not only obliged to remove the unlawful content but also has to take all technically feasible and reasonable precautions to prevent future infringements.[152] Thus, a specific (in terms of the Federal Court of Justice: not a general!) monitoring obligation is initially triggered as soon as the provider obtains notice of unlawful third party content.[153] The existence and extent of specific monitoring obligations largely depend upon the circumstances of the individual case, in particular upon the feasibility of measures after taking into account economic and technical reasonableness.[154] In practice, a specific monitoring obligation of this kind forces pro-active monitoring on to providers, this being the only way they can comply with court orders to prevent infringements of third parties' rights in the future. There is indeed much legal uncertainty about the specific duties of the provider. The German Federal Court of Justice has ruled that the extent of such obligations has to be assessed by the court with jurisdiction for questions of enforcement (in a separate procedure) regarding the imposition of disciplinary fines for culpable non-compliance with an injunction (see § 890 ZPO). Furthermore, the monitoring obligation is not restricted to a specific piece of illicit content or activity but rather, covers all infringements that appear to be essentially *similar* to the original infringement (so-called "Core -Theory"). Hence, every piece of content or activity that appears similar to the one incriminated has to be blocked and banned by the provider. Thus, this extension results in a sort of general monitoring obligation – limited to similar infringements, but nevertheless rather broad.

The **Austrian** Supreme Court of Justice upheld a claim for refraining from defamations of business reputation (§ 1330 (2) ABGB), on the grounds that the operator of an online guestbook had violated an obligation to examine. Claims according to § 1330 ABGB require the *unlawfulness* of the dissemination of facts, which is as a rule indicated where personal honour and business reputation are affected. However, the unlawfulness can be excluded on the grounds of legal justification in cases where the behaviour complained of can be considered legitimate in the light of a comprehensive consideration of all interests involved. Weighing up the factors of freedom of speech and personal honour and economic reputation,

[152] GE12. – BGH, 11/3/2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I.
[153] GE15. – OLG München, 21.9.2006, 29 U 2119/06, MMR 2006, 739 (740).
[154] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I; GE 6. – OLG Hamburg, 22.8.2006, 7 U 50/06, MMR 2006, 744 (746) - heise.de; GE 8. – OLG Düsseldorf, 7.6.2006, I-15 U 21/06, MMR 2006, 618 (619 f.) ; GE 15. – OLG München, 21.9.2006, 29 U 2119/06, MMR 2006, 739 (740).

the court held that the balance of interests would turn to the disadvantage of the operator of the online guestbook where an examination obligation has been violated. A general obligation to examine the process of posting articles was excluded as being incompatible with § 18 (1) ECG (= Art. 15 (1) ECD) and moreover as unduly restricting the constitutional freedom of speech. The court however regarded an obligation to examine as being reasonable where the operator had obtained *notice of at least one infringement so that the danger of further infringements by individual users was substantiated*. Due to the violation of the obligation to examine the defamations committed by users could be attributed to the operator of the guestbook; his behaviour was therefore unlawful.

In **Italy** Article 17, para. 3 of the Legislative Decree No. 70 (implementing the EDC) holds that an access provider is liable (in terms of civil liability) for the content of the services defined in article 17, para. 2, (b) if, having been requested to do so by the judiciary or administrative monitoring authority, he fails to act promptly to block access to such content or if, having been informed that the content of a service to which he controls access is of an illegal nature or is detrimental to a third party, he fails to inform the competent authority. Some stakeholders (e.g. telecommunications companies and ISPs) have requested the European Commission to take action against Article 17, para. 3, as not being consistent with Art. 15 ECD.[155]

In the **UK** there had been concern about a potential conflict between the prohibition of general monitoring obligations and the obligation to remove repeat publications under the Terrorism Act 2006[156]. According to section 3 (4) to (6) a person who has been given a notice is to be regarded as having endorsed any future *re-publication* of a statement that is the same or to the same effect as the original statement (so-called "repeat statement") *unless* he has taken every reasonable step to prevent re-publication *and*, once aware of the publication, has taken every reasonable step to remove it. The new Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007[157] which creates specific exemptions from liability for offences under sections 1 and 2 of the Terrorism Act for intermediaries providing mere conduit, caching or hosting services, now takes into account article 15 ECD. According to the DTI's explanatory memorandum "the effect of the exceptions from liability in regulations 5 to 7 is that intermediaries could not be required to comply with any such general obligation arising from subsections (4) to (6) of section 3 of the Terrorism Act".[158]

II. Injunctions by Civil Courts

Obviously, the bulk of court decisions across Europe concern injunctions against providers. However, the impact of these injunctions on providers' liability (and responsibility) is difficult to assess since their extent and the legal reasoning behind them depend largely on the

[155] Letter dating from October 2, 2006 from the AIIP (Italian Association for Internet Providers to the European Commission.
[156] http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en.pdf.
[157] Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 (SI 2007/1550), available at: http://www.opsi.gov.uk/SI/si2007/20071550.htm.
[158] See the DTI explanatory memorandum, No. 4.7.

particular legal grounds on which the injunction was based. Specific provisions for injunctions, as in copyright law or trademark law, may apply as well as general legal doctrines, such as on the law of tort in Germany. Moreover, some jurisdictions obviously concentrate on preliminary injunctions embedded in civil procedure codes whereas other jurisdictions provide for preemptive injunctions as "stand-alone" claims which can be filed without e.g. claiming damages (as in Germany). For the purpose of this study, we have to note however that hardly any comprehensive study is available that gives details of the various treatments of injunctions in Europe and their basis in law.

1. Specific Provisions for Injunctions Against Intermediaries

Some jurisdictions provide explicitly for injunctions in their copyright acts, trademark laws, or other specific legal rules on protection of rights (press law, privacy protection etc.). Whereas the full coverage of all these specific injunctions is beyond the scope of this study one legal area does merit specific interest: the (for some Member States still pending) implementation of Article 8 (3) InfoSoc-Directive[159], and Article 11 Enforcement Directive[160] which require that Member States provide for an injunction to prohibit the continuation of the infringement, both against the actual wrongdoer and against intermediaries whose services are used by a third party for the infringements.

One example is **Sweden**: Here § 53 b of the Swedish Copyright Act has been amended as part of the incorporation of Art 8 InfoSoc Directive, and now states that an injunction may also be issued against a party contributing to an infringement in an objective sense, without any need to show intent or negligence. As far as access providers are concerned a committee is currently working on possible powers to issue injunctions against providers if their services are used for infringing copyright (without any obligation to show that they have contributed to the infringement). Moreover, even if Section 5 of the **Swedish** Act on Responsibility for Electronic Bulletin Boards is not a legal basis for injunctions, it still stipulates a statutory obligation to erase unlawful messages mentioned in the Act. Sec. 5 presupposes an infringement of certain provisions of the Swedish penal code (such as inciting rebellion, agitation against a national ethnic group, child pornography) or copyrights or other rights protected by Section 5 of the Copyright (Artistic and Literary Works) Act (1960:729) which is "obvious" to the operator of the bulletin board.

In the field of copyright law, the **UK** High Court has power to grant an injunction against an information society service provider, but only where that service provider has actual knowledge of another person using its service to infringe copyright (section 97A of the Copyright Designs and Patents Acts 1988[161]). In determining whether a service provider has

[159] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ 167/10 of 22.6.2001.
[160] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ of 30.4.2004 157, 45.
[161] Copyright and Related Rights Regulations 2003, Statutory Instrument 2003/ 2498. The regulation implements InfoSoc-Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ 167/10 of 22.6.2001.

actual knowledge for the purpose of this section, a court shall take into account all matters which appear to it in the particular circumstances to be relevant and, amongst other things, shall have regard to whether a service provider has received a notice through a means of contact made available in accordance with regulation 6(1)(c) of the E-Commerce Regulations and the extent to which any notice includes the full name and address of the sender of the notice, details of the infringement in question (sections 97A(2) of the Act; the provision is similar to Regulation 22 of the E-Commerce Regulations).[162]

In addition the **Austrian** Copyright Act provides for a special legal basis for injunctions against intermediaries in § 81 (1a) UrhG after they have been given a warning. In fact most of the civil court injunctions have been based on intellectual property law like copyright and trademark law, but also on competition law.

In contrast, given the principles of "accessory liability" (Störerhaftung) the **German** Government has seen no necessity to expressly incorporate Art. 11 3rd Sentence of Directive 2004/48/EC into German law. In fact in a large number of cases injunctions have already been based on those principles.[163]

In Article 1.6 of Law No. 128 of May 21, 2004 (implementing the Decree of March 22, 2004, No. 72 – the so-called UrbaniDecree) **Italian** law explicitly also provides in cases of copyright infringements for an obligation on the part of host providers (but not access providers) to remove or block access to contents if requested by a judicial authority competent to issue such an injunction.[164]

Similarly, **French law** stipulates in Art. 6.1.8. of the LCEN/France[165] that injunctions can be granted ordering the shut-down of a whole web site or the blocking of access to the incriminated web site, together with the right to order the provider to take technical steps to make further diffusion impossible. Furthermore, Article 6.I-8 has to be compared with Article 8 which can only be used for copyright issues. Art 6.I-8 has a larger scope as more categories of infringements are concerned; more categories of actions can be taken as not only stopping infringements is possible but also preventing infringement is possible.

2. Injunctions based on general norms and legal doctrine; preconditions for injunctions against internet intermediaries

In most cases intermediaries such as providers of discussion fora, auction platforms or internet access are not, by merely providing their service, involved in infringements as actual wrongdoers but rather as causal contributors (helpers) to the infringement committed by another person – usually the content provider or user of his service. However, we have to note that in some cases direct infringement and mere secondary contribution can hardly be

[162] See Part 1:A.III.3.c)bb)

[163] See Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (Entwurf der Bundesregierung vom 24.01.2007), BR-Drucks. 64/07, p. 70, 75, for an extensive description see Country Report Germany Part 1 A. I.

[164] Article 1.6 of the Italian Law No. 128 of May 21, 2004, which has converted the decree March 22, 2004, No. 72 – the so-called Urbani Decree.

[165] This article uses a subsidiarity principle, see the Country Report for France and above Part 1:B.I.2.

distinguished and injunctions have been issued against intermediaries as direct infringers of copyright as in the **Danish** Tele2 vs. IFPI case.[166]

Probably the most far-reaching doctrine of contributory "liability" in the case of injunctions has been developed by **German** courts, which base injunctions against intermediaries on a relatively strict legal doctrine called "accessory liability" (Störerhaftung).[167] According to this doctrine it is not only the wrongdoer himself (direct infringer)[168] and participants (effective promoters or helpers[169]) that can be subject to a claim for termination of and refraining from infringements, but also mere accessories. Consequently responsibility for unlawful content in principle is extended to all persons who – without necessarily being wrongdoers or participants – deliberately and generally causally contribute to the infringement of a third party's right, provided they have the legal and effective means of preventing the infringement.[170] However, because accessory liability should not be extended unreasonably to third parties who did not commit the infringement themselves, they may only be held liable where there was a duty on their part to examine the actions or contents of third parties.[171] The extent of this so-called *duty to examine* is subject to a rule-of-reason-test and depends on the function and activity of the possible accessory as well as the individual responsibility of the direct infringer. The reasonableness of examination is subject to criteria like knowledge of a clear infringement, provocation of third-party infringements through prior activities (e.g. articles) on the part of the provider or the private or commercial character of the service.[172] Non-profit-making services are widely exempted from such duties to examine, such as Domain Name Registrars, which are deemed to act in the social interest.[173] Moreover, the character of the service in question and its similarity to press or broadcasting services that uphold the freedom of speech and the liberty of the press have to be taken into account.[174]

Similarly the **Austrian** Supreme Court of Justice (Oberster Gerichtshof – OGH) held, with regard to injunctions, that an intermediary could only be held liable as a *contributor* when he had assisted in the infringement of a right by the actual wrongdoer. Such a contribution

[166] DE1. – City Court of Copenhagen, 25/10/2006, *Tele2 vs IFPI,* http://resources.tele2.dk/privat/pdf/tele2_ke.pdf.
[167] See for an extensive description of the principles of accessory liability the Country Report for Germany Part. 1, A. I.
[168] The person who commits an infringing actions himself.
[169] I. e. persons who deliberately encourage another person to commit an infringement, or who deliberately contribute to an infringement committed by another person.
[170] *Köhler*, in: Hefermehl/Köhler/Bornkamm, § 8 UWG Rn. 2.12.
[171] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I (auction platform); GE13. – BGH, 19.4.2007, I ZR 35/04, MMR 2007, 507 - Internetversteigerung II (auction platform); GE35. – BGH, 17.5.2001, I ZR 251/99, MMR 2001, 671 – ambiente.de (domain name registry); BGH, 18.10.2001, I ZR 22/99, GRUR 2002, 618 – Meißner Dekor.
[172] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I; GE35. – BGH, 17.5.2001, I ZR 251/99, MMR 2001, 671 – ambiente.de; GE6. – OLG Hamburg, 22.8.2006, 7 U 50/06, MMR 2006, 744 – heise.de; GE15. – OLG München, 21.9.2006, 29 U 2119/06, MMR 2006, 739; GE8. – OLG Düsseldorf, 7.6.2006, I-15 U 21/06, MMR 2006, 618: the court found that no duty to examine existed, particularly stressing the non-commercial character of the service (proceeding: LG Düsseldorf, 6.7.2006, I-15 U 21/06).
[173] GE35. – BGH, 17.5.2001, I ZR 251/99, MMR 2001, 671 – ambiente.de.
[174] GE6. – OLG Hamburg, 22.8.2006, 7 U 50/06, MMR 2006, 744 – heise.de.

presupposes that the intermediary had failed to prevent an infringement "*obvious to a non-lawyer without further investigation*".

Courts in other member states do not seem to have not developed such detailed, explicit tests.

3. Preliminary Injunctions (Procedural Injunctions) versus Permanent Injunction (pre-emptive injunctions)

Closely related to the relationship between general monitoring obligations and injunctions is the question of whether injunctions are to be granted according to civil procedure codes or on grounds of "stand-alone" claims: Some Member States provide for independent actions of injunction, others seem to concentrate more on preliminary (temporal) injunctions considered to be a mere part of a claim for damages (or other claims) or of criminal procedure, in order to prevent "faits accomplis", i.e. not to jeopardize the final outcome of the proceedings.

In **Germany** in particular, there is a clear distinction between a claim for injunctive relief according to substantive law on one hand and the procedural enforcement of such a claim on the other hand. The plaintiff may either seek a judgment ordering the defendant to cease further infringements or apply for a preliminary injunction, which is in principle an interlocutory measure. Injunctions by German civil courts are independent of criminal law or claims for damages; in other words, a right holder may apply for an injunction against a provider (in order to block illicit content in the future) without filing an action for damages. Consequently, an injunction can be granted even though a claim for damages is barred by the exemptions of §§ 8 to 10 TMG. Thus, the injunction is by no means a temporary measure (merely connected to the outcome of the main claim) but rather a lasting, and in theory perpetuated obligation for the future independent of the fate of the main action (which might be an action for damages).

In contrast, **Italian** courts seem to concentrate on claims for preventive remedies (*domanda cautelare*)[175] according to Article 700 of the Italian Civil Procedure Code.[176] According to this article the court is entitled to issue its ruling with or without hearing the parties, after ruling on whether *fumus boni iuris* (the preliminary evidence that the application is well-founded) and *periculum in mora* (the risk involved in delay) exist, and in order to restrain a party from persisting with a course of conduct until the case has been decided.

The potential conflict between preliminary injunctions according to civil procedural codes, which should be limited in time, and general pre-emptive injunctions based on substantive law (and actions), like in Germany, is reflected in the Aargh case in **French** law: The French Supreme Court will have to decide to what extent such an injunction could be ordered if the request for an injunction were to be embedded in another claim (e.g. for damages). The Court

[175] It may be useful to remind the reader of the meaning of the Italian procedural term *domanda cautelare*, which describes an application made by the principal petitioner requesting the defendant to stop behaving in a wrongful manner whilst awaiting trial decision. The use of this *preventive* remedy is therefore only temporary in order to avoid the risk of irreparable damage

[176] IT7. – Court of Bari June 13, 2006.

of Appeal stated that even if injunctions were based on preliminary actions according to the civil procedural code they could be unlimited as to time.[177]

4. Injunctions against Specific Types of Providers

a) Mere Conduit

Injunctions by civil courts concentrate on blocking access to file-sharing systems or to distributors of illicit contents. First, we have to distinguish two types of cases: contributory infringement and direct infringement.

One case which has been reported from **Denmark** concerns a direct infringement of intellectual property rights: In *Tele2 vs IFPI* an access provider (Tele2) was ordered by the court to block the access to a website housing copyright infringing MP3 files.[178] However, the Copenhagen court based the decision on the fact that the access provider had copied, although only for milliseconds, MP3 files on its routers, and thus found the access provider guilty of violating the copyrights on its own account. For this reason, the access provider was declared liable for the contents transmitted. The court, however, did not take into account either the ECD nor Art. 5 of the InfoSoc-Directive[179], which states that ephemeral copies do not constitute a violation of copyright.

However, the bulk of cases in Member States concern injunctions in the context of contributory infringements by access providers: A European precedent in this field is the well-known **Belgian** case of 'Sabam v. Tiscali'[180] which dealt with p2p software and the issue of copyrights. The judge expressly acknowledged the existence of a cause of action (*action en cessation*) against an intermediary (here: the access provider) even if he was not directly the author of the infringement. However, the question of the technical feasibility for a mere conduit provider to filter traffic data and actively to search for copyright infringements was deliberately left open by the judge of first instance, who felt himself technically unqualified to deal with this question without expert advice. The onus of proof was laid on the plaintiff, who nevertheless succeeded in producing expert evidence that technical measures were indeed feasible. Consequently, the Belgian judge[181] in June 2007 ordered the mere conduit provider Scarlet (formerly Tiscali) to put in place filtering measures to prevent copyright

[177].FR1. – TGI Paris, 20/04/2005, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, http://www.juriscom.net/jpt/visu.php?ID=684, http://www.juriscom.net/documents/resp20050627.pdf; FR2. – TGI Paris, 13/06/2005, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1139 , http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf; FR3. – CA Paris, 24/11/2006, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1139, http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf.

[178] DE1. – City Court of Copenhagen, 25/10/2006, Tele2 vs IFPI, http://resources.tele2.dk/privat/pdf/tele2_ke.pdf.

[179] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ 167/10 of 22.6.2001.

[180] BE3. – Tribunal de première instance de Bruxelles (cessation), 26.11.2004, *R.D.T.I.*, 2005, liv. 21, p. 89, note E. Montero, Y. Cool, n° 04/8975/A, (SABAM c. Tiscali).

[181] BE6. – Tribunal de première instance de Bruxelles, 29.06.2007, (SABAM c. Scarlet), N° 04/8975/A, *inédit*.

infringements, on the basis of the expert advice that had been put before the court. The judge expressly refuted the defendant's argument that filtering tools would result in a general monitoring obligation (and thus would contradict Art. 15 ECD). The judge upheld that injunctions (actions en cessation) are not affected by Art. 15 ECD or Art. 12 ECD. Moreover in the judge's view, the measures identified by the expert (like for instance "Audible Magic" (CopySense Network Appliance): a solution facilitating the identification of protected musical files prone to p2p interference) — are technical instruments with limited action to block or filter particular material on the network but without imposing any general monitoring obligation. Furthermore - according to the judge's reasoning – Scarlet would not lose its liability exemption applicable to mere conduit as it would not take any active part in the filtering: no information transmitted via Scarlet would be modified (note: modification or amending content would argue against mere conduit status and therefore jeopardise the liability exemption of Art. 12 ECD).[182]

In a recent decision in **Germany** LG Frankfurt am Main issued a preliminary injunction against an access provider ordering the blocking of access to the website "youporn.com".[183] The injunction had been applied for by the operator of a German porn website who saw a violation of competition law since the youporn website did not include an age-verification-system and in addition contained child porn content.

Likewise **Dutch** copyright associations sued access providers for granting access to P2P-networks or to software distributors: In *Stichting Brein vs KPN*,[184] the Court of The Hague recently ordered KPN as access provider to cut off its client's access to the internet completely (!) by cutting the ADSL-connecting lines, based on a "duty of care doctrine" arising from copyright law and obliging access providers to protect authors rights and to stop third party infringements. The client had hosted on his servers a bittorrent website that infringed copyrights. The further implications of this case are still unclear, and it remains to be seen if the decision will be followed by other courts.

The courts are however in general unhappy when asked to suspend completely access to the internet, at least in summary proceedings. Thus, the President of the **French** TGI of Paris declared that he was not qualified to judge whether the rescission of contract was required to stop the access.[185] Article 6.I-8 LCEN to which reference was made uses the formula "prevent damage or stop damage" and the judge made a stringent and rigorous interpretation of it.

In contrast, the **UK** Queens Bench Division deemed an injunction against access providers (in this case AOL, Tiscali and British Telecommunication) to be disproportionate; moreover, no sufficient prior notice had been given to the providers.[186] The case concerned the (further)

[182] BE6. – Tribunal de première instance de Bruxelles, 29.06.2007, (SABAM c. Scarlet), N° 04/8975/A, *inédit.*
[183] LG Frankfurt am Main, 2-06 O 477/07, the official text of the decision is not yet available.
[184] NE6. – Court of The Hague, 05/01/2007, Stichting Brein vs KPN, LJN number AZ5678, case number 276747/KG ZA 06-1417, accesible via www.rechtspraak.nl.
[185] FR6. – TGI Paris, 08/10/2004, ord. Sur requête, 3ème Chambre, Société Civile des Producteurs Phonographiques c/ Wanadoo, www.forumInternet.org/telechargement/documents/tgi-par20041008.pdf.
[186] UK1. – Queen's Bench Division, 10/3/2006, [2006] EWHC 407 (QB); [2006] 3 All ER 336; [2006] EMLR 523, Bunt v Tilley & Others.

dissemination of defamatory material. According to the decision the injunctive relief sought by the plaintiff in the case was entirely disproportionate to any conceivable legitimate advantage. The plaintiff apparently had applied for an order preventing any supply of services to the individual responsible for the defamatory postings. According to the court this would be draconian and pointless, since such services could be obtained with great ease elsewhere. Even if the claim for an injunction had been restricted to prevent the publication of defamatory words, the court held this would be unworkable and disproportionate since the defendants did not host any material and had no ability or power to amend or modify any content.

In **Spain** injunctions against access providers seem to be limited to orders by competent authorities such as the Commercial Tribunal de Madrid[187] which have applied the liability exemption of Art. 14 of the Spanish LSSICE to injunctions (in a case regarding copyright infringements), in particular to preliminary and preventive injunctions (as provided by Spanish e-commerce law and copyrights law). Desisting from an illegal activity or the removal of illicit content could then only be ordered if it was required by the general duty of cooperation of the mere conduit provider (Article 11 LSSICE[188]).

b) Host Providers

Prominent examples of injunctions issued by civil courts are provided by a number of German and Austrian decisions at the highest level. The **Austrian** Supreme Court granted an injunction against a provider who operated an internet forum (called "online guest-book") in which a third party published defamatory messages.[189] Weighing up questions of freedom of speech, personal honour and economic reputation, the court held that a monitoring obligation is reasonable if the web site operator (host provider) had obtained notice of at least one infringement so that the danger of further infringements by individual users was substantiated. Hence, the operator of the guestbook was obliged to constantly monitor if new statements/defamations of the same kind has been placed on the server (in the guest-book). The court took into account the fact that the plaintiff was unable to file suit against the author of the defamation (being anonymous) and that the defendant was likely to face further infringements, since the original article invited further similar statements by other (anonymous) users. The court held that checking specific infringements should be possible with considerably less effort than conducting general monitoring.

[187] SP1. – Commercial Court of Madrid n° 2, 10.11.2004, (Emi Music v. Bitmailer), n° 14/2004.
[188] Article 11. - Duty of cooperation of intermediary service poviders.
"1. When a body competent in the field has ordered, in the exercise of the duties legally conferred on them, that the provision of an information society service be stopped or that certain content from providers established in Spain be taken down, and the cooperation of the intermediary services providers is necessary to this, it shall be able to order these providers, directly or by means of a request submitted to the Ministry of Science and Technology, to suspend transmission, data storage, access to the telecommunications networks or the provision of any other equivalent intermediary service that they undertake."
[189] AU5. – OGH, 21/12/2006, 6 Ob 178/04a (Online – Gästebuch), http://www.internet4jurists.at/entscheidungen/ogh6_178_04a.htm.

In another decision the **Austrian** Supreme Court of Justice[190] held a provider to be assisting unfair competition and stated that the infringement was so obvious that even a non-lawyer could detect it without further investigation. However, the court held also that the host provider had no obligation to make inquiries concerning the alleged illegality of a website after obtaining notice from the plaintiff.

The online-guestbook case of the Austrian Supreme Court is paralleled by a **Polish** case in which the trial court[191] held that a host provider (deemed to be the "publisher" of an online discussion forum) had to check the comments in the forum before "publication" – which has been largely criticised as running counter to Art. 14 APSEM.

In **Germany**, the decisions against internet auction platforms such as eBay or (formerly) Ricardo based on contribution to trademark infringements are worthy of note together with other decisions dealing with providers of online discussion forums hosted by online press publishers. As described above, German courts apply the traditionally wide notion of "accessory liability" (Störerhaftung).[192]. However, in order to restrict the wide scope of such liability, German courts use a specific test with regard to obligations to examine and monitor (third party) content. The German Federal Court of Justice has obliged the auction platform (host provider) in general to monitor its websites for future infringements of a similar kind as the auction platform cannot be compared to a non-profit-making organisation which profits from a generous liability exemption. However, the courts have conceded that the assessment of reasonable monitoring obligations might be difficult in specific cases and might depend on technical and economic feasibility. The business model should not be endangered by these monitoring obligations. The definition of such monitoring obligations is thus deliberately left to the enforcement procedure.

In **Belgium** host providers have been ordered to remove illicit content; for example one provider (*in solidum* with the website's owner) was required to remove defamatory terms and expressions, in which a number of Belgian priests were likened to paedophiles, from a website he hosted. They (the host provider and the website owner) were also ordered to disseminate the decision on the "Actualité" rubric of the website[193]. This decision was prior to the ECD implementation. During another lawsuit, the plaintiff and the host provider reached an out-of-court settlement providing that the intermediary should expressly and irrevocably remove and prohibit the defamatory content.[194] Before the implementation of the ECD into Belgian law, the courts had already held providers of a Bulletin Board System liable for third party content which had infringed copyright. Subsequently, the intermediary had been required to monitor the BBS users.[195]

---

[190] AU6. – OGH, 6/7/2004, 4 Ob 66/04s (megasex.at), http://www.internet4jurists.at/entscheidungen/ogh4_66_04s.htm.
[191] PO1. – Sąd Rejonowy w Słupsku, 7/3/2007, sygn. akt II 342/06; not yet available.
[192] See Country Report Germany Part. 1 A. I.
[193] BE11. – Liège (*réf.*), 28 nov. 2001, *J.T.*, 2002, liv. 6051, pp. 38 et s., note A. CRUQUENAIRE ET J. HERVEG.
[194] BE12. – Tribunal de première instance de Bruxelles (référé), 2.3.2000, A.M., 2001, pp. 147 et s., note M. Isgour, (Monsieur M. O. c. P.Y. L. et c. Belgacom Skynet).
[195] Cour d'appel d'Anvers, 28 févr. 2002, *A.M.*, 2002, pp. 340 et s., first instance : Tribunal de première instance d'Hasselt, 16 févr. 1999, *A.M.*, 1999, pp. 287 et s.

In **Spain**, an intermediary was considered liable for defamatory content hosted on his mirror website and was required to desist from his illegal activity (by removing defamatory expressions) and to disseminate this on his website. Surprisingly, the host provider's legal exemptions were not referred to.[196] The appeal decision[197], contrary to the first judgment, referred to the host provider's legal exemptions. Nevertheless, the liability exemption was not excluded by the judge on the grounds that the intermediary had actual knowledge of the illicit content. He therefore endorsed the host provider's liability and upheld the injunctions.

Several **Dutch** Courts have also ordered injunctions against host providers. In *Lycos vs Pessers*[198], the injunction obliged the provider to reveal date and details of clients. In XS4ALL vs DB[199], the court ordered the host provider to block access to a website hosting contents related to terrorism. The most prominent case, however, is the decision in *Stokke BV vs Marktplaats BV*:[200] Here the court explicitly referred to the German decision in Ricardo.de (or Internet-Versteigerung I), stating that injunctions are not affected by the liability exemptions of the ECD. Hence, hosting providers have a "duty of care" to prevent and terminate infringements, the court did not however distinguish between a duty of arising care prior to or following notification of such infringements (as German courts do). The court clarified the link between liability and notice and take-down procedure; such a procedure (complaint page and take-down afterwards) was held to be sufficient to meet the standards of care which the court developed for market-place operators, weighing up the profits and losses of the parties against the secondary role of market-place operators.[201] The court explicitly took into account the prohibition of general monitoring obligations as stated by Art. 15 ECD. The Court acknowledged that technically it is very difficult for the host provider to do more, in particular to establish a filtering mechanism.[202] Hence, the court dismissed an ex ante obligation of the market operator to control its websites. The Court compared the expenses for doing more and came to the conclusion that these would be too costly compared to the stated aim of such procedures, contained in the references of the ECD to voluntary notice-and-take-down-procedures.

---

[196] SP6. – Decision (*Sentencia*) n° 00126/2005, Court of first Instance of Madrid (n° 42), June 15th 2005 – SGAE (*Sociedad General de Autores y Editores*) v. *Asociación de Internautas*.

[197] SP7. – Provincial Court of Madrid (Section 19), February 6th 2006, appeal decision n° 841/2005 –*Asociación de Internautas* v. SGAE (*Sociedad General de Autores y Editores*).

[198] See NE11. – 13 – District Court of Haarlem, 11/09/2003, Lycos Netherlands BV vs Mr Pessers, LJN number AL1882, case number 94609/KG ZA 03-426, available via www.rechtspraak.nl; Appeals Court of Amsterdam, 24/06/2004, Lycos Netherlands BV vs Mr Pessers, confirmed by the Supreme Court, 25/11/2005, Lycos Netherlands BV vs Mr Pessers, LJN number AU4019, case number C04/234HR, available via www.rechtspraak.nl;.

[199] NE17. – Gerechtshof Amsterdam, 07/11/2002, XS4ALL vs Deutsche Bahn AG, LJN number: AF0091, case number: 762/02 SKG, available via www.rechtspraak.nl .

[200] NE 15. – District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, disponible via www.rechtspraak.nl; see also NE 16. – District Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, accessible via www.rechtspraak.nl - which, however, does not deal with the duty of care doctrine.

[201] Note that this line of reasoning has not been restricted by the courts to injunctions.

[202] However, note, that the court based its reasoning upon the defendants arguments (Marktplaats) as it deemed the arguments of Stokke not be substantiated sufficiently. There had been no expertise ordered by the court, such as in the belgium case SABAM.

In **France**, injunctions against host providers hosting illegal online gambling operators have been applied: The Tribunal de Grande Instance of Paris[203] had for instance to deal with an online gambling site based in Malta. The Court decided to apply the French law because the players were located in France. The Court ordered the (foreign) host provider to stop hosting the illegal website (according to Art. 6.I-8 LCEN). The Court also stated that the gaming activity was manifestly illegal and that the LCEN regime was applicable. This ruling was subsequently overturned by the Court of Cassation. The Supreme Court endorsed the ECJ teachings of the Gambelli and Placanica cases, deciding that where French gaming laws restrict free movement of services, lower courts must verify whether these restrictions comply with the requirements set by article 49 of the Rome Treaty. The Supreme Court also required from lower courts that they check whether general interest is guaranteed in the Member State where private operators are established.

Italian courts have not yet had to decide specific claims for injunctions against host providers. However, in one case before the Court of Bari, plaintiffs asked for a removal of their own pictures from the defendant's hosted website. The court allowed the claim for preventive remedies (*domanda cautelare*)[204] according to Art. 700 of the Italian Civil Procedure Code.[205] According to this article the court is entitled to issue its ruling with or without hearing the parties, after ruling on whether *fumus boni iuris* (the preliminary evidence that the application is well-founded) and *periculum in mora* (the risk involved in delay) exist, and in order to restrain a party from persisting with a course of conduct until the case has been decided.

In other member states injunctions against intermediaries are being currently discussed, as in **Sweden** (mentioned already), regarding actions directed at providers hosting web sites which contain copyright infringements.[206]

III. Administrative Orders

1. General Issues

Specific legal provisions on injunction are seldom to be found: **Portugal** has enacted a specific provision in sec. 18 (2) of the Portuguese E-commerce Law[207] stipulating that any interested party can bring a complaint against a host provider or a network content aggregation provider (by means of search engines, hyperlinks or similar procedures), before the competent authority: the latter has 48 hours to make a decision and to notify it to all

[203] FR50. - TGI Paris, 02/11/2005, G.I.E. PMU c/ Computer Aided Technologies Limited et Bell Med Limited, http://www.foruminternet.org/telechargement/documents/tgi-par20051102.pdf;
FR51. - CA Paris, 14/06/2006, Computer Aided Technologies Limited et Bell Med Limited c/ G.I.E. PMU, http://www.foruminternet.org/telechargement/documents/ca-par20060614.pdf.

[204] It may be useful to remind the reader of the meaning of the Italian procedural term *domanda cautelare*, which describes an application made by the principal petitioner requesting the defendant to stop behaving in a wrongful manner whilst awaiting trial decision. The use of this *preventive* remedy is therefore only temporary one in order to avoid the risk of irreparable damage

[205] Court of Bari June 13, 2006

[206] See also below for § 53b of the Swedish Copyright Act.

[207] Art. 18 of the Law Decree n° 7 /2004, 07.01.04.

parties concerned. The authority is designed according to its competences. ANACOM (Communications National Authority) is the competent authority by default.

Germany provides for a legal basis for administrative orders against all kinds of telemedia services pursuant to §§ 8 to 10 TMG (mere conduit, caching and hosting) and in § 59 of the revised Interstate Agreement for Broadcasting and Telemedia (Rundfunkstaatsvertrag – RStV[208]), which became effective on 1.3.2007. This regulation is referred to in § 20 (4) of the Interstate Agreement on the Protection of Minors Concerning Telemedia Services (Jugendmedienschutz-Staatsvertrag – JMStV[209]) which assigns the task of enforcing the protection of minors to the State Media Authorities represented by the Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz der Landesmedienanstalten – KJM).

In **Spain** Articles 8 and 11 of the Spanish e-commerce law require from intermediaries particular duties of cooperation with the competent judicial or administrative authority in order to stop a violation: If the provider of an information society service established in a foreign country infringes the following principles – public order, criminal investigations, public security and national defence; public health; dignity and of the principle of non-discrimination; youths and children – the competent judicial or administrative authority may order the intermediaries to take appropriate measures in order to block access to the illicit content (Article 8 Spanish e-commerce law). If the provider of an information society service violating these principles is established in Spain, the competent authority may require intermediaries to take the appropriate measures according to their general duty of cooperation provided by the article 11 of the e-commerce Spanish law. For instance, the Spanish Ministry of Industry, Commerce and Tourism administrative decision[210] required, on the basis of Article 8 of the Spanish e-commerce law, that mere conduit providers registered at the National Commission of Telecommunications Market prevent access to an incriminated website (www.losburrales.com) whose provider was not established in Spain.

Article 11 of the Spanish e-commerce law provides the general duty of cooperation by intermediaries :"When a body competent in the field has ordered, in the exercise of the duties legally conferred on them, that the provision of an information society service be stopped or that certain content from providers established in Spain be taken down, and the cooperation of the intermediary services providers is necessary to this, it shall be able to order these providers [...] to suspend transmission, data storage, access to the telecommunications networks or the provision of any other equivalent intermediary service that they undertake."

Italy goes further than merely stating the law on injunctions in that it actively requires access providers to block access to websites that disseminate specific contents. Thus, the Italian law

[208] Staatsvertrag für Rundfunk und Telemedien (Rundfunkstaatsvertrag – RStV) vom 31.8.1991, zuletzt geändert durch Art. 1 des Neunten Staatsvertrages zur Änderung rundfunkrechtlicher Staatsverträge vom 31.7. bis 10.10.2006 (GBl. BW 2007 S. 111).
[209] http://www.kjm-online.de/public/kjm/downloads/JMStV.pdf
[210] SP2. – Administrative Decision of the Ministry of Tourism, Industry and Commerce, 28.07.2006, LSSI/06/046.

on Gambling[211] entitles the Autonomous Administration of State Monopolies (AAMS) to communicate to access providers the list of the sites in which someone offers games or bets where money can be lost or won without having the authorisation that is usually granted by AAMS itself, thus obliging the providers to block those web-sites. Moreover, the Italian act on Child Pornography[212] requires ISPs in general (mostly access providers, but also host providers) to report to the national centre for the prevention of Internet child pornography if they become aware of these facts. After reporting, ISPs (and hence access providers) are expected to keep such materials for at least 45 days, and – following the so-called Gentiloni Decree[213] - are obliged to block (filter) access to all websites listed and communicated by the above mentioned national centre within 6 hours after receiving due notice.[214] The Act dated February 6, 2006, No. 38 provides for technological measures required for ISPs to be established by a decree of the Ministry of Communication and the Ministry for Reforms and Innovations in Public Administration. The Gentiloni Decree regulates further details, for example that ISPs must be equipped to block out prohibited sites according to requirements set out in such provisions, that is within 60 days after the publication of the decree in the Official Gazette for the relevant "domain name" and within 120 days starting from the same date for the relevant "IP address". Outcomes, technologies and conformity with the intentions of the law are to be checked over every six months.

2. Orders against Specific Types of Providers

a) Mere Conduit

German administrative courts have endorsed orders issued by state authorities[215] against access providers by ordering them to block access to Nazi propaganda websites. The Higher Administrative Court of Münster (Oberverwaltungsgericht - OVG) confirmed these injunctions as a suitable means to obstruct the proliferation of Nazi propaganda in Germany.[216] The court considered the order to be reasonable and proportionate since the blocking of the content was technically feasible.[217] It was left to the provider to find the appropriate technical means to accomplish this task.[218] In particular, the court took a

[211] Article 50 and 51 of the Law December 27, 2006, No. 296 (Financial Law for 2007).
[212] Article 14 of the Law No. 269 of 1998.
[213] Art. 3, this decree was passed on January 2, 2007, and it is entitled "Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet devono utilizzare al fine di impedire l'accesso ai siti segnalati dal Centro nazionale per il contrasto della pedopornografia", http://www.comunicazioni.it/it/index.php?IdPag=1177.
[214] Some stakeholders stressed that the decree does not indicate when the Centre is expected to provide ISPs with the list of the websites. According to these stakeholders, this could cause problems for ISPs, because it takes time to put legal provisions into practice and to put filters in action, cf. Country Report Italy.
[215] Regional Administration of Duesseldorf.
[216] GE1. – OVG Münster, 19.3.2003, 8 B 2567/02, MMR 2003, 348 – Düsseldorfer Sperrverfügungen.
[217] VG Arnsberg, 6.12.2002, 13 L 1848/02 (court of lower precedence to OVG Münster, 19.3.2006, 8 B 2567/02, MMR 2003, 348 - Düsseldorfer Sperrverfügungen); VG Köln, 3.3.2005, 6 K 7151/02, MMR 2005, 399; VG Düsseldorf, 10.5.2005, 27 K 5968/02, MMR 2005, 794; VG Minden, 31.10.2002, 11 L 1110/02, MMR 2003, 135 VG Düsseldorf, 19.12.2002, 15 L 4148/02, MMR 2003, 205.
[218] GE1. – OVG Münster, 19.3.2003, 8 B 2567/02, MMR 2003, 348 (351).

favourable view of the technical means suggested by the state authorities such as blocking of IP-addresses, modification of domain-name-servers and use of proxy-servers.[219]

However, it should be noted that in another administrative case concerning the arrangement and broking of gaming offers, the Bavarian Higher Administrative Court (Bayerischer Verwaltungsgerichtshof – BayVGH) held that there are no appropriate means to filter and to block inhabitants of Bavaria from obtaining access to gaming offers.[220] For particular legal reasons the injunction was forced to concentrate on blocking access for inhabitants of Bavaria: there was no jurisdiction to block the access to the websites in general. The court expressly stated that there is currently no software or technical means available to spot the location of an internet user. A provider could not therefore be ordered to use location-based filtering. In addition the onus of proof for the practicability of the measures ordered was laid upon the authority, which initially had argued that it was up to the gambling provider to investigate whether the order was feasible. In contrast to the proceedings before the Bavarian court, in the case before the OVG Münster the blocking of DNS-addresses by access providers and other measures seemed to be undisputedly technically feasible; the Regional Administration of Düsseldorf was therefore entitled to leave it to the access provider to find suitable means.

Similarly, in **Spain**, the Ministry of Industry, Commerce and Tourism Administrative Decision[221] required mere conduit providers registered with the National Commission of Telecommunications Market to prevent access to an incriminated website (www.losburrales.com). The Ministry had previously been required[222] to take appropriate measures against these intermediaries. The administrative resolution did not specify the reasons for which the website "www.losburrales.com" had to be blocked. The decision was based on Provision 8.1 LSSICE authorising the competent authorities to take appropriate measures to restrict an information society service for: a) the protection of public order, criminal investigations, public security and national defence, b) the protection of public health, c) the protection of the dignity and of the principle of non-discrimination, d) the protection of young people and children[223].

b) Host Providers

In contrast to access providers, injunctions issued (and published) by state authorities/agencies are rare. In **Portugal** two administrative resolutions ordering injunctions against host providers are reported. However, they are only preliminary injunctions and

[219] GE1. – OVG Münster, 19.3.2003, 8 B 2567/02, MMR 2003, 348 (351).
[220] BayVGH, 7.5.2007, 24 CS 07.10, published at juris.de
[221] SP2. – Administrative Decision of the Ministry of Tourism, Industry and Commerce, 28.07.2006, LSSI/06/046.
[222] Decision of the Examining Magistrate of Torrelavega, May 22nd, 2006; not available
[223] Concerning the protection of young people, the State Prosecutor's Office Order n° 2/2006, of March 15th lays down the level of collaboration required from ISPs in accordance with Article 8.1 of the LSSICE. When the State Prosecutor has the knowledge of a content infringing paragraph d) above, he notifies the Internet Service Provider involved and he orders removal of the illicit content. The State Prosecutor's order is sufficient to establish the intermediary's "actual knowledge" (compare: Articles 16 and 17 LSSICE).

provisional resolutions of conflict, and thus not fully comparable to injunctions in other member states. The Portuguese injunctions were based on Article 18 (2) of the Portuguese e-commerce law[224]. The first such administrative resolution[225] forced a host provider to remove the incriminated website from the network. The decision also required intermediary service providers associated with illicit content to disable access to the website. The second administrative resolution[226] has also imposed on host providers and on intermediary service providers associated with content an obligation to block access to a website that infringes copyrights. These resolutions (the first one of which is very brief and the second not available) do not offer further details.

As regards **anti-terrorism measures,** some member states go far beyond these obligations, like the **UK** in its Terrorism Act 2006. Sections 3 and 4 of the Terrorism Act 2006[227] establish a notice and take-down regime under which a police constable can issue a notice[228] requiring the removal from public view, or the amendment of, a statement, article or record which the constable considers to be "unlawfully terrorism-related". The hosting provider must comply with the notice within a specified period of time (2 working days). Failure to fulfil this obligation is an offence and could result in criminal charges against the hosting provider in question and its directors. In June 2007 the Terrorism Act was amended by the Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007.[229] Regulations 5 to 7 of these Regulations incorporate Art. 12 to 14 ECD and create specific exemptions from liability for offences under sections 1 and 2 of the Terrorism Act for intermediaries providing mere conduit, caching or hosting services. After the Regulations have come into force, hosts are only required to take down specified unlawfully terrorism-related material following receipt of a notice; they are not obliged to look out for and take down "repeat statements" pursuant to sections 3(4) to (6) of the Act.[230]

IV. Measures Issued

Where injunctions ordering to refrain from infringements have been issued against intermediaries by civil courts in **Germany**, these courts grant a general order to refrain from further infringements, but without further specification of the technical means of how to achieve this goal, for example the use of filter software. This issue is left to the discretion of the providers.[231] Furthermore the feasibility of using filter software has been one of the

[224] Art. 18 of the law decree n° 7 /2004, 07.01.04.
[225] PR1. – Administrative decision from the National Authority of Communications (ANACOM) – 18.05.04 – Case Nokia Portugal v. Verza Facility Management, Google and others.
[226] PR2. – Administrative decision from the General Inspection of Cultural Activities – 2005.
[227] http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en.pdf.
[228] See Part 1:A.III.3.c)bb) above for details on notices under section 3 of the Terrorism Act.
[229] Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 (SI 2007/1550), available at: http://www.opsi.gov.uk/SI/si2007/20071550.htm.
[230] We have received a statement on this issue from the Department of Trade and Industry (DTI), see also Part 1:B.I.3.
[231] See for example GE20. – LG Berlin, 13.1.2005, 27 O 573/04, MMR 2005, 785.

criteria when assessing the reasonableness of obligations to examine as a precondition to the granting of an injunction on the basis of the principles of accessory liability.[232]

In the decision "Internetversteigerung I" the German Federal Court of Justice[233] contemplated the use of special filter software to fulfil a duty to examine with regard to trademark infringements on an auction platform, but ultimately left it up to the provider to find adequate technical means.[234] In "Internetversteigerung II" the court found it beyond dispute that eBay was to a certain extent able to apply filtering software which following the giving of certain keywords would detect suspicious offers; these would then have to be examined manually.[235] Neither decision goes into technical details. As can be seen, there is some legal uncertainty about the specific obligations of the intermediary until the court competent for enforcement matters finally decides on the imposition of a disciplinary fine in the event of contempt of court.

In a recent civil case in Germany dealing with an access provider[236], the injunction ordering blocking of a porn website apparently did not order any specific technical measures and the access provider decided to comply with the order by applying so-called DNS-blocking, i. e. the exclusion of domains in the domain-server, thus ensuring that queries would not be forwarded to the pornographic website in question. Initially the provider had relied on blocking IP addresses, but since this method resulted in the additional blocking of harmless websites, he decided to apply DNS-blocking which had also been contemplated by the Regional Administration of Düsseldorf in cases dealing with Nazi propaganda. In the wake of this decision the DNS-blocking technique became a matter of controversy in computer expert circles since it is said to be easily circumvented. In the "Düsseldorfer Sperrverfügungen" case dealing with administrative blocking orders, the OVG Münster however dismissed such concerns: as blocking would impede access to the website for a large number of users it was not decisive to the court that other users could still easily circumvent the blocking and reach the respective websites.[237]

However, in another administrative case concerning the arrangement and broking of gaming offers the Bavarian Higher Administrative Court (Bayerischer Verwaltungsgerichtshof – BayVGH) held that there are no appropriate means to filter and to block inhabitants of Bavaria from obtaining access to gaming offers.[238] The court expressly stated that there are currently no software or technical means available to spot the location of an internet user. Consequently location-based filtering could not be ordered against a provider.

---

[232] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I; GE13. – BGH, 19.4.2007, I ZR 35/04, MMR 2007, 507 – Internetversteigerung II; GE14. – BGH, 12.7.2007, I ZR 18/04; GE15. – OLG München, 21.9.2006, 29 U 2119/06, MMR 2006, 739; GE4. – LG München I, 19.4.2007, 7 O 3950/07, MMR 2007, 453; GE10. – LG Berlin, 10.11.2005, 27 O 616/05.

[233] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I

[234] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I; see also GE15. – OLG München, 21.9.2006, 29 U 2119/06, MMR 2006, 739 (741).

[235] GE13. – BGH, 19.4.2007, I ZR 35/04, MMR 2007, 507 – Internetversteigerung II.

[236] LG Frankfurt am Main, 2-06 O 477/07, the official text of the decision is not yet available.

[237] GE1. – OVG Münster, 19.3.2003, 8 B 2567/02, MMR 2003, 348 – Düsseldorfer Sperrverfügungen.

[238] BayVGH, 7.5.2007, 24 CS 07.10, until now only published at juris.de

In sum, the following technical measures have been endorsed by **German** administrative courts[239] and deemed suitable by German administrative authorities:

- The exclusion of IP-addresses by blocking in the router

  A router may be configured in a way that the entire data communication to a specific IP-address will not be forwarded.

- The exclusion of domains in the domain-server (DNS)

  Where an access provider operates a DNS, it may be configured in a way that queries are not forwarded to the right server, but an invalid or another pre-defined website.

- The use of proxy servers.

  The URL (Uniform Resource Locator) is the precise criterion for the allocation of an individual website on a particular server. By using proxy-servers the URL can be blocked. A query for illicit information will either be filtered out and access denied or it will be re-routed to a pre-defined website in the browser

Where courts in **Belgium** and **Spain** ordered intermediaries to remove illicit content or to disable access to certain websites, the relevant technical measures have not been specified.[240] In the Belgian case of Sabam vs. Scarlet the court left it to the provider to choose the adequate technical filtering measures to stop copyright infringements on a p2p platform. Scarlet has six months to communicate to Sabam the technical measures it will take to stop the copyright infringements.[241]

For **Italy** the statute on on-line betting and gambling activities mentioned above is normally put into practice by hijacking DNS communication and redirecting it to the DNS server of the AAMS. Users trying to access such websites instead receive a notice saying that "Pursuant to the decree of the AAMS of 7 February 2006, regarding the removing of on-line gambling games without the proper authorization (article 1 par. 50 and 51 Law 27 December 2006, No. 296), the requested website is not accessible because it does not have the necessary authorizations for collecting bets in Italy. The list of the authorized operators is available on the institutional website www.aams.it". Furthermore, the *Gentiloni*- decree contains two different ways of filtering. Notably, the Ministry of Communications decided that ISPs must be equipped to block out prohibited sites according to requirements set out in the decree itself,

[239] GE1. – OVG Münster, 19.3.2003, 8 B 2567/02, MMR 2003, 348 (351).

[240] Cf. Belgian cases : BE6. – Tribunal de première instance de Bruxelles, 29.06.2007, (SABAM c. Scarlet), N° 04/8975/A, *inédit*; BE15. – Tribunal de première instance de Bruxelles (cessation), 5.9.2006, www.droit.be, n° 2006/9099/A, (CopiePresse c. Google); BE11. – Cour d'appel de Liège (*réf.*), 28.11.2001, *J.T.*, 2002, liv. 6051, pp. 38 et s., note A. Cruquenaire et J. Herveg, (J.A. et a.s.b.l. Evêché de Liège c. Association Nopedo « Touche pas à mes enfants », a.s.b.l. Religion raëlienne de Belgique, M. L., L.V.); BE 13. – Tribunal de première instance d'Hasselt, 16.2.1999, *A.M.*, 1999, pp. 287 et s., (Affaire Novell & ministère public c. C). BE8. – Tribunal de commerce de Bruxelles (cessation), 2.11.1999, *A.M.*, 1999, pp. 474 et s., n° 2192/99, (IFPI Polygram Records c. SA Belgacom Skynet) and the Spanish cases SP6. – Decision (*Sentencia*) n° 00126/2005 of the Court of first Instance of Madrid (n° 42), June 15th, 2005 – *SGAE* (*Sociedad General de Autores y Editores v. Asociación de Internautas* ; SP7. – Decision (*Sentencia*) of the Provincial Court of Madrid (Section 19), February 6th 2006, Appeal request n° 841/2005 – Affaire *Asociación de Internautas* v. *SGAE* (*Sociedad General de Autores y Editores*) ; SP10. – Decision (Auto) of the Examining Magistrate of Madrid (n° 3), August 1st, 2003, n° 5741/2002 – « EDonkey ».

[241] BE6. – Tribunal de première instance de Bruxelles, 29.06.2007, (SABAM c. Scarlet), N° 04/8975/A, *inédit.*

that is, within 60 days after the publication of the decree in the Official Gazette for the relevant "domain name" and within 120 days starting from the same date for the relevant "IP address". Outcomes, technologies and conformance with purposes of the law are to be checked every six months.

C. General Monitoring Obligations

I. Statutory Monitoring Obligations

Some member States do not have any doctrine of duty to monitor, either abstract or general; examples are Denmark,[242] Finland, Spain, Ireland and the Netherlands.[243] Hence, they have seen no need to implement the exclusion of general monitoring obligations (Art. 15 ECD). Other member states explicitly referred to Art. 15 (1) ECD by stating that general obligations to monitor are excluded, like the UK.[244] Other member states have incorporated Art. 15 ECD verbatim, leading sometimes to a review of already existing statutes, as in Luxemburg. Article 63, § 2 of the Luxembourg E-commerce Law required host providers to monitor specific contents (e.g. relating to child pornography). This provision was held to be inconsistent with the exclusion of general monitoring obligations and was repealed by the Law of December 18th, 2006.

The absence of a general monitoring obligation is sometimes expressly endorsed by the courts, such as in Italy by the Court of Milan[245] in a case of child pornography in which the public prosecutor had sued both the "editor" of the web-site and the host provider, in defiance of the norms relating to publisher liability (art. 57 and 57 (2) of the Italian Criminal code). The court found that host providers are not liable for wrongful acts committed by third parties (i.e. content providers) as long as their role is limited to hosting websites.

Similarly the **German** Federal Court of Justice found that a general obligation on the part of the operator of an auction platform to examine all offers prior to their publication on the internet was unreasonable since it would jeopardise the whole business model.[246] According to the **Austrian** Supreme Court of Justice a general obligation to examine the process of posting articles was denied as being incompatible with § 18 (1) ECG (= Art. 15 (1) ECD) and would moreover unduly restrict the constitutional freedom of speech.[247] By contrast a **Polish** trial court[248] held that the operator of an online discussion forum had to check the comments

[242] Act N° 227 of 22 April 2002 on information society services, including certain aspects of electronic commerce, available via http://www.forbrug.dk/english/laws/4/ .
[243] Parliamentary documents of the Dutch Lower House 2001/02, 28 197, N°3, p. 27. Can be found using www.overheid.nl/op .
[244] „Guide for Business to the Electronic Commerce (EC Directive) Regulations 2002 (SI 2002/2013)" (p. 28) http://www.dti.gov.uk/files/file14635.pdf.
[245] March 18, 2004.
[246] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I.
[247] AU5. – OGH, 21/12/2006, 6 Ob 178/04a (Online – Gästebuch), http://www.internet4jurists.at/entscheidungen/ogh6_178_04a.htm.
[248] PO1. – Sąd Rejonowy w Słupsku, 7/3/2007, sygn. akt II 342/06, official text not yet available.

in the forum before "publication" – this has been widely criticised as being inconsistent with Article 14 APSEM.

One notable exception[249] to Art. 15 ECD –representing the inherent potential conflict between Recital 48 of the ECD and Art. 15 ECD – is the **Swedish** Law for Electronic Bulletin Boards (Act on Responsibility for Electronic Bulletin Boards (1998:112)[250] which imposes on bulletin board operators a general obligation to control and to monitor the content of their websites. The Swedish Government explicitly refers to recital 48 of the ECD that had been inserted on the recommendation of the Swedish government during the drafting of the ECD. Whereas the Act was originally supposed to refer to small networks (of Bulletin Boards), its definitions are so wide that its scope of application tends to encompass a large number of electronic services on the web that are also dealt with by the E-Commerce-Directive.[251] In particular, the operator of a Bulletin Board is obliged at all times proactively to monitor his website – and not only after he has received notice of an infringement. Hence, he is obliged to monitor the service regularly and in a fashion and to an extent that may reasonably be required taking into consideration the scope and nature of the service. It is a criminal offence to fail to remove such illegal content from the bulletin board, if such failure is intentional or grossly negligent. Failure is punished by fines, or if regarded as serious, by imprisonment for up to two years.

However, it is important to note how Swedish practice applies these apparently wide notions. Even where the host is presumed to have some knowledge of the posted content[252], he does not need to monitor every message, but rather to carry out regular checks. In no event should the service be left unchecked for more than a week. However, if there are too many messages in relation to his capacity to supervise the bulletin board, it has been reported that he might comply with his obligations by way of installing a complaint page where users might report any irregularities. In practice, this seems to be the way the monitoring obligation is usually fulfilled.[253] There are not however any court decisions on these Bulletin Board obligations. In sum, Swedish practice seems to apply a form of notice and-take-down procedure, in contrast to the apparently strict wording of the Bulletin Board Act.

II. Monitoring Obligations due to Court or Administrative orders

As pointed out before, court orders or administrative orders, in particular injunctions, can effectively result in an obligation to monitor a service, and thus almost amount to a general monitoring obligation. Dependent on the doctrine applied in individual countries, a specific monitoring obligation may apply not only to the specific content of an infringer/tortfeasor but

[249]Concerning other specific monitoring obligations arising out of specific regulations concerning anti-terrorism acts, gambling acts or child pornography acts, see the corresponding chapter (host providers etc.).

[250] Lag om ansvar för elektroniska anslagstavlor, Unofficial translation by the government available under: http://www.sweden.gov.se/content/1/c6/02/61/42/43e3b9eb.pdf

[251]For the exact wording and content of the BBS Act, see in detail the Swedish Country Report.

[252] Government bill on the Act on Responsibility for Electronic Bulletin Boards, page 15 (Prop 1997/98:15, s 15).

[253]We have received information on this issue from the Swedish Ministry of Justice and the law firm Mannheimer Swartling.

to all similar infringements of the same kind, the so-called "core theory" of German courts in cases of intellectual property rights or unfair competition.[254] In view of the problems involved in automatically filtering out illicit content such an obligation may prove to almost amount to a general monitoring obligation.

D. Communication and Cooperation Obligations

Communication and cooperation obligations need to be distinguished from monitoring obligations. Both are closely connected to each other but are not the same: Whereas monitoring obligations may lead either to obligations to communicate/report or at least to remove illicit content without request, communication obligations may only come into play when an authority or a private party request the provider to disclose information.

Internet Intermediaries are subject to a number of communication- and cooperation obligations that can be divided into four rough categories:

- Obligations to Actively Inform Public Authorities;
- Obligations to Provide Information at Request of Public Authorities;
- Obligations to Provide Assistance for Interception by Public Authorities;
- Claims for Disclosure of Information brought by private right holders.

Closely connected to the provision of information are data retention obligations for this purpose. In a broader sense compliance with administrative and judicial orders etc. could also be summarized under the term cooperation obligations. Obligations to block or remove unlawful content and prevent future infringements have however already been dealt with separately.

Member states' national legislation provides for communication and cooperation obligations for intermediaries in a great variety of areas such as telecommunication law, intellectual property law, codes of criminal procedure and so on. In addition requests for information by public authorities and private right holders alike have to be embedded in the broader context of data protection law, as recently shown by the attorney general of the European Court of Justice in the case *Promusicae vs. Telefonica*.[255] The legal situation consequently tends to be rather complex.

I. Obligations to Actively Inform Public Authorities

Obligations to actively inform public authorities may either arise from specific provisions where intermediaries are expressly mentioned or from general provisions of criminal law, which however only apply to serious crimes and not for example to mere copyright infringements. In practice many intermediaries voluntarily communicate information on detected illegal activities to the competent authorities.

[254] See in extenso Country Report Germany Part. 1 A. I. 2. b) and II. 2..
[255] Conclusions of the Advocate General Juliane Kokott of 18.7.2007, Case C-275/05, Productores de Música de Espana (Promusicae) v Telefonica de Espana SAU.

According to Article 15 (2) ECD "member states may establish obligations for intermediaries promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by their recipients […]". One group of member states, Belgium[256], Cyprus[257], Estonia[258], France[259], Greece[260], Italy[261], Latvia[262], Lithuania[263], Malta[264] and Portugal[265] provide for a special obligation on the part of intermediaries to communicate illegal activities or information on their services. Whereas most countries stick to the words of Art. 15 (2) ECD and include illegal activities and information in general, the **French** regulation in Article 6-I-7 (3, 4, 5) LCEN restricts itself to offences cited in the fifth and eighth paragraphs of article 24 of the Act of 29 July 1881 on the freedom of the press and article 227-23 of the French Penal Code. Thus, if internet intermediaries have been notified of illicit activities violating public interests like crimes against humanity, racism, child pornography, or contents that suggest violence or violate human dignity (article 6-I-7, alinéa 3, 4 et 5) they are obliged to report these activities to the authorities. Moreover, internet intermediaries have to install technical equipment to ensure that they may receive such notifications and have to inform the public about the methods in question.

Some member states deviate slightly from the words of the directive and in addition require "actual knowledge" or "awareness" of the illegal activities[266], but there have been no reports of the practical consequences of this.

In particular the **Belgian** law imposes a reporting obligation on caching and host providers towards the public prosecutor (procureur du Roi) where it has actual knowledge of illicit activities or contents (Articles 19 (5) & 20 (3), Law on certain legal aspects of information society services of 11 March 2003). Mere conduit, caching and host providers alike are obliged to inform the competent legal or administrative authorities of alleged illegal activities that recipients of their services may be committing or alleged illegal information that the latter may be providing (Article. 21 (2) Law on certain legal aspects of information society services of 11 March 2003).

In **Italy, in addition to** Article 17 (2) of the Legislative Decree no. 70 of 9 April 2003, the act against child pornography[267] stipulates a legal obligation to report to the "National Centre

[256] Article. 19 No. 5, 20 (3) Law on certain legal aspects of information society services of 11 March 2003.
[257] Section 18 Framework Law No. 156 (I) of 2004 on certain aspects of information society services, in particular electronic commerce, and related matters.
[258] § 11 (3) Act on Information Society of 14 April 2004 (Riigi Teataja 2004, 29, 191).
[259] article 6-I-7 (3, 4, 5) LCEN.
[260] article 14 (2) Presidential Decree 131 of 16 May 2003.
[261] article 17 (2) Legislative Decree no. 70 of 9 April 2003.
[262] § 11 (1) Information Society Services Law published in OJ No. 183 of 17 November 2004
[263] Article 15 (1) Law on information society services of the Republic Lithuania of 25 May 2006 (Nr. X-614).
[264] Provision 22 Electronic Commerce Act (Chapter 426) of 10 May 2002 (Act No. III of 2001, as amended by Act No. XXVII of 2002.
[265] article 13 (a) of Law- Decree No. 7/2004 of 7 January 2004 (Diário da republica I-A n° 5 de 7/1/2004 p. 70.
[266] BE20. - Cour de cassation, 3.2.2004, *R.D.T.I.*, 2004, n° 19, n° P.03.1427.N, (V.R. c. ministère public); FR6. – TGI Paris, 08/10/2004, ord. Sur requête, 3ème Chambre, Société Civile des Producteurs Phonographiques c/ Wanadoo, http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=838 http://www.foruminternet.org/telechargement/documents/tgi-par20041008.pdf .
[267] Article 14 of the Law of August 3, 1998, No. 269 "Exploitation of child prostitution, child pornography and child sex tourism as new forms of slavery".

for the Fight Against Child Pornography on the Internet" companies and subjects that distribute, disseminate or trade child pornographic materials. ISPs have a duty to report if they become aware of these facts. After having reported, intermediaries are expected to keep the materials in question for at least 45 days (article 14 of the Law No. 269 of 1998 "Exploitation of child prostitution, child pornography and child sex tourism as new forms of slavery").[268]

Other member states like **Austria**, the **Czech Republic**, **Germany**, **Hungary**, **Poland, the Slovak Republic** and **Sweden** do not provide for obligations for providers to give information of illegal behaviour without administrative request. The national criminal codes of the majority of member states make it an offence not to notify certain committed or intended offences to the public authorities.[269] **Poland** provides for a general social obligation to inform the competent enforcement authorities about certain type of crimes (i. e. crimes which are prosecuted ex officio);[270] however, this obligation is only of a social and not a legal nature, so non-observance does not have any legal effects. These obligations however are mostly restricted to the most serious crimes and are consequently of little relevance for internet intermediaries.

II. Obligations to Provide Information at Request of Public Authorities

Member states' legal systems give the legal basis for obligations to provide information at the request of public authorities. In Article 15 (2) ECD the directive itself mentions "obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their services with whom they have storage agreements". According to member states' legal systems, requests for information by public authorities are not restricted to host providers, but may also be directed towards mere conduit and caching providers. In fact requests for disclosure of information on the identity of internet users, for example in Austria and Germany, have largely involved access providers.

Decisions relating to requests for information by public authorities have (often) referred to the identification of holders of dynamic IP-addresses for purposes of criminal prosecution. The offences in question have mainly involved punishable infringements of copyrights in file-sharing cases.

Since under the existing **German** law claims for information against intermediaries are a matter of dispute and usually disallowed by courts, complaints that a punishable offence has been committed are used by copyright holders or collecting societies to force the authorities to

[268] Intermediaries are obliged to block (filter) the access to all websites listed and communicated by the above mentioned national centre within 6 hours of receiving due notice : see Art. 3 of the so-called *Gentiloni*-decree (Requisiti tecnici degli strumenti di filtraggio che i fornitori di connettività alla rete Internet devono utilizzare al fine di impedire l'accesso ai siti segnalati dal Centro nazionale per il contrasto della pedopornografia of 2.1.2007, available at http://www.comunicazioni.it/it/index.php?IdPag=1177).

[269] Austria: § 286 StGB; Germany: § 138 StGB; Poland: Art. 303 § 1 Polish Code of Criminal Procedure Ustawa z dnia 6 czerwca 1997 roku Kodeks Postępowania Karnego (Dz.U. z 1997 roku Nr 89, poz. 555; Hungary: for example § 175/A Btk; Slovak Republic: § 340 Act No. 300/2005 Z.z.; Sweden: Penal Code (1962:700), chapter 23, section 6).

[270] Art. 303 § 1 Polish Code of Criminal Procedure Ustawa z dnia 6 czerwca 1997 roku Kodeks Postępowania Karnego (Dz.U. z 1997 roku Nr 89, poz. 555).

identify the names and addresses of copyright infringers, so that the information can be used in subsequent civil legal action.

1. Legal Basis of Requests

Amongst member states Austria[271], Belgium[272], Cyprus, France[273], Greece[274], Italy[275], Latvia[276], Lithuania[277], Malta[278] and Portugal have incorporated Art. 15 (2) ECD into their national acts implementing the E-Commerce Directive.

Austria has explicitly implemented Art. 15 (2) ECD in § 18 (2) and (2) ECG, but even went beyond the specifications of this directive, as § 18 (2) ECG covers not only host providers (§ 16 ECG) but also mere conduit providers (§ 13 ECG).

Similarily in **Latvia,** § 11 (2) of the Information Society Services Law published in OJ No. 183 of 17 November 2004 is not restricted to host providers, but covers all kinds of intermediaries.

In **Austria,** § 18 (2) ECG provides that both mere conduit and host providers are obliged to inform courts authorised by law for this purpose about user identities for purposes of criminal prosecution. § 18 (3) contains an obligation for host providers to inform authorities about the names and addresses of recipients of their services. However, the actual legal basis for a request for information arises from regulations in Austrian substantive law like the Code of Criminal Procedure (e. g. § 149a Code of Criminal Procedure (Strafprozessordnung 1975 – StPO)[279]), the Industrial Code (Gewerbeordnung 1994) or the Securities Trading Act (Wertpapierhandelsgesetz).[280] In a case dealing with the communication of the name and address of the user of an (already known) dynamic IP-address the Austrian Supreme Court held that the information could informally be communicated to the court under § 103 (4) TKG 2003.[281]

In contrast to Art. 15 (2) ECD, Article 14 (2) of the **Greek** Presidential Decree 131 of 16 May 2003 (Government Gazette Volume I, No 116) makes a general reservation in favour of the "protection of privacy" and the "protection of personal data". "protection of privacy" refers mainly to the privacy of telecommunications[282], which is protected at both constitutional level under the ordinary law (Law 2225/1994, P.D. 47/2005).

[271] § 18 (2) and (3) ECG.
[272] article 21 (2) Law on certain legal aspects of information society services of 11 March 2003
[273] article 6-II LCEN Art. 6-II LCEN.
[274] article 14 (2) Presidential Decree 131 of 16 May 2003 (Government Gazette Volume I, No 116)
[275] article 17 (2) Legislative Decree no. 70 of 9 April 2003.
[276] § 11 (2) of the Information Society Services Law published in OJ No. 183 of 17 November 2004
[277] article 15 (2) Law on information society services of the Republic Lithuania of 25 May 2006 (Nr. X-614).
[278] Provision 22 Electronic Commerce Act (Chapter 426) of 10 May 2002(Act No. III of 2001, as amended by Act No. XXVII of 2002).
[279] Kundmachung der Bundesregierung vom 9. Dezember 1975
über die Wiederverlautbarung der Strafprozeßordnung 1960 (Strafprozeßordnung-StPO) BGBl 1975/631.
[280] 817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP, zu § 18, available at http://www.parlinkom.gv.at/pls/portal/docs/page/PG/DE/XXI/I/I_00817/daten_000000.doc.
[281] OGH, 26.7.2005, 11 Os 57/05z, 11 Os 58/05x, 11 Os 59/05v.
[282] Article 19 of Greek Constitution; Law 2225/1994, Presidential Decree 47/2005.

Member states that have not introduced any regulation incorporating Art. 15 (2) ECD do not seem to feel any hindrance in applying general rules regarding requests for information. Requests can be based on the codes of criminal procedure of the member state in question, the police laws, or the telecommunication laws etc. In many member states possible grounds for requests for information extend across a number of different regulations resulting in a complex legal situation.

The **UK** imposes in specific cases obligations to report communication details to the authorities, e.g. in compliance with a warrant issued under Section 5(1)(a) of the Regulation of Investigatory Powers Act 2000 to secure the interception of a communication in the course of its transmission by means of a telecommunication system.

In **Germany**, decisions relating to requests for information by public prosecutors have mainly referred to the identification of holders of dynamic IP-addresses. German courts have predominantly applied § 113 TKG and consequently rejected the necessity of a judicial order as required by §§ 100g, 100h StPO, since the disclosure of the name and address of the holder of an already known IP address only referred to customer data, not to traffic data protected by confidentiality of telecommunications (§ 88 TKG, Art. 10 GG).[283]

In **Italy**, besides the above-mentioned active reporting obligation,[284] intermediaries are also obliged to report to the National Centre for the Fight Against Child Pornography on the Internet upon request any information relating to agreements entered into with entities or individuals that provide child pornography. The provision aims at preventing anonymous activities (Article 14 of the Law August 3, 1998, No. 269 "Exploitation of child prostitution, child pornography and child sex tourism as new forms of slavery"). Moreover, courts may require the cooperation of intermediaries in the event of copyright infringements under the Italian Law of May 21, 2004, No. 128.[285] According to this regulation intermediaries must communicate to the police all information they have that can be useful for the identification of the content providers or of the persons who have committed copyright infringements. The information may however be communicated only following request by the judicial authority (article 1 (6) Law of May 21, 2004, No. 128).

2. Data Protection

As mentioned above, requests for information against intermediaries mostly relate to names and addresses of users of dynamic IP addresses who had allegedly been involved in illegal activities. In Austria and Germany such requests for information have raised the question of restricting details of names and addresses of holders of IP addresses to the terms of the data

[283] Applying § 113 TKG: LG Stuttgart, 5.11.2004, 9 Qs 80/04, NStZ-RR 2005, 218; LG Stuttgart, 4.1.2005, 13 Qs 89/04, MMR 2005, 624; LG Hamburg, 23.6.2006, 631 Qs 43/05, MMR 2005, 711; LG Würzburg, 20. 9. 2005, 5 Qs 248/05, NStZ-RR 2006, 46. Applying §§ 100g, 100h StPO: LG Ulm, 5.10.2003, 1 Qs 1088/03, MMR 2004, 187.

[284] Cf. Part 1:D.I.

[285] Incorporating the Decree of March 22, 2004, No. 72 – the so-called *Urbani*-Decree[285] –, which modified Italian copyright law).

categories of data protection law, and consequently the additional question of the general preconditions and boundaries for the disclosure of such information.

With regard to the name and address of the user of a dynamic IP address the **Austrian** Supreme Court of Justice ruled that the communication of the name and address of the user of an (already known) dynamic IP address was not subject to the strict preconditions stipulated in § 149a StPO, but could informally be communicated to the court pursuant to § 103 (4) TKG 2003 since the request for information only referred to customer data.[286]

Similar to the decision of the Austrian Supreme court, the **German** courts have predominantly applied § 113 TKG (not §§ 100g, 100h StPO) and consequently rejected the requirement of a judicial order, hold that the disclosure of the name and address of the holders of an already known IP address merely related to customer data, not to traffic data protected by the principle of confidentiality of telecommunications (§ 88 TKG, Art. 10 GG).[287]

However, now that the **Advocate General at the European Court of Justice** has concluded that the disclosure of the names and addresses of holders of dynamic IP-addresses constitute disclosure of traffic data protected by telecommunication privacy directives,[288] the Austrian and German courts are expected to reconsider their position.

III. Obligations to Provide Assistance for Interception by Public Authorities

Member states provide for specific obligations to provide assistance for interception by public authorities. In most member states intermediaries must comply with these obligations at their own expense. These obligations refer to access providers that are also providers of telecommunications services, and are usually set out in the telecommunications legislation as well as in special acts regulating the relevant national authorities such as intelligence agencies or the police. This area of the law is rather complex and varies from state to state.

IV. Claims for Disclosure of Information

Apart from injunctions against providers in order to block access or remove illicit content, actions for disclosure of information about users are quite frequent in Europe and filed mainly by copyright holders or associations in file-sharing cases. The claims mainly dealt with the disclosure of the names and addresses of recipients of services allegedly involved in infringements of intellectual property rights and have been mainly directed against access providers and operators of auction platforms, but also of search engines. Private actions are also closely related to restrictions on disclosure of information due to data protection law.

[286] OGH, 26.7.2005, 11 Os 57/05z, 11 Os 58/05x, 11 Os 59/05v.
[287] Applying § 113 TKG: LG Stuttgart, 5.11.2004, 9 Qs 80/04, NStZ-RR 2005, 218; LG Stuttgart, 4.1.2005, 13 Qs 89/04, MMR 2005, 624; LG Hamburg, 23.6.2006, 631 Qs 43/05, MMR 2005, 711; LG Würzburg, 20. 9. 2005, 5 Qs 248/05, NStZ-RR 2006, 46. Applying §§ 100g, 100h StPO: LG Ulm, 5.10.2003, 1 Qs 1088/03, MMR 2004, 187.
[288] Conclusions of the Advocate General Juliane Kokott of 18.7.2007, Case C-275/05, Productores de Música de Espana (Promusicae) v Telefonica de Espana SAU.

1. Legal Basis for Claims

The most relevant legal basis for claims for information are the individual national laws on intellectual property rights such as the copyright or trademark acts.

Austria stipulates in § 87b (3) UrhG a right for copyright holders to demand information against intermediaries in copyright infringement cases. Based on this provision an Austrian court granted the music industry a right to claim from access providers information concerning the name and address of the holder of an IP address.[289] In a decision regarding a provider of value-added telephone numbers, the Supreme Court granted a concerned party a right to claim information about the identity of potential infringers on the grounds of an analogous application of § 18 (4) ECG[290]; this decision could well become relevant for internet access providers as well.

In contrast to the Austrian courts, **German** courts have not usually acknowledged any right to force a provider to disclose the names and addresses of users who had allegedly committed copyright infringements. The claims for information have been based on § 101a Copyright Act (Urhebergesetz – UrhG)[291] which requires the plaintiffs to establish that the person he sues for the disclosure of information was indeed involved in the infringement of the plaintiff's copyrights. § 101a UrhG is restricted to copyright infringements through the manufacture (§ 16 UrhG) or distribution (§ 17 UrhG) of copies. For several reasons the requirements of § 101a UrhG have not been met in these German cases.[292] Furthermore, especially in cases related to host providers, the courts have rejected claims for information on the grounds that data protection provisions did not give providers the right to disclose data to holders of intellectual property rights.[293]

In a number of cases[294] **Dutch** courts have imposed upon access providers the obligation to provide third parties (copyright holders) with details of their clients. However, it is hard to deduce any principle as the Supreme Court emphasised that it had pronounced any such general rule in the case of *Lycos v. Pessers*. Notwithstanding these reservations, the Court of The Hague set out to develop a general "duty of precaution and of due diligence" in order to

[289] AU2. – HG Wien, 21/6/2006, 18 Cg 67/05, http://www.internet4jurists.at/entscheidungen/hg67_05w.pdf.
[290] AU3. – OGH, 16/3/2004, 4 Ob 7/04i, http://internet4jurists.at/entscheidungen/ogh4_7_04i.htm
[291] Gesetz über Urheberrecht und verwandte Schutzrechte of September 9, 1965, BGBl. I S. 1273.
[292] See in extenso the German Country Report GE2. – OLG Frankfurt, 25.1.2005, 11 U 51/04, MMR 2005, 241; GE3. – OLG Hamburg, 28.04.2005, 5 U 156/04 MMR 2005, 453.
[293] GE11.. – KG, 25.9.2006, 10 U 262/05, MMR 2007, 116.
[294] Provisional measures, NE4. – Judge of Utrecht, 12/07/2005, Stichting Brein and others vs UPC Nederland BV and other isp's , LJN number AT9073, case number 194741/KGZA 05-462, accessible via www.rechtspraak.nl , upheld by NE5. – Appeals Court of Amsterdam, 13/07/2006, Stichting Brein and others vs UPC Nederland BV and other isp's, LJN number AY3854, case number 1457/05KG, availableble via www.rechtspraak.nl; NE11. – 13 – District Court of Haarlem, 11/09/2003, Lycos Netherlands BV vs Mr Pessers, LJN number AL1882, case number 94609/KG ZA 03-426, available via www.rechtspraak.nl; Appeals Court of Amsterdam, 24/06/2004, Lycos Netherlands BV vs Mr Pessers, upheld by the Supreme Court, 25/11/2005, Lycos Netherlands BV vs Mr Pessers, LJN number AU4019, case number C04/234HR, available via www.rechtspraak.nl; NE6. – Court of The Hague, 05/01/2007, *Stichting Brein vs KPN* LJN number AZ5678, case number 276747/KG ZA 06-1417, accessible via www.rechtspraak.nl.

oblige the access provider to disclose data on its clients; data protection norms have not been discussed. This duty was based on the general liability provisions of Dutch copyright law.[295]

In an **Italian** case concerning copyright infringements via P2P networks a record company sued several access providers pursuant to article 156bis of the Copyright Act, demanding the name and the addresses of the peer-to-peer systems users (the claim was however dismissed by the court of appeal on data protection grounds).[296]

In **France**, a court obliged the access provider „Free" to disclose the identification data of users to a plaintiff on the grounds of violation of trademark law, but, only following judicial request.[297] Similarly both the courts of the TGI Paris[298] and the Court of Appeal[299] held that an access provider has to disclose any data concerning the authors of racist contents (hosted on foreign web servers operated by a third party); however, the appeal to the Supreme Court has not yet been decided. Court orders to disclose the relevant data of clients of providers (i.e. authors) are based largely on Art. 6 II LCEN which imposes an obligation to store such data and disclose them on order of the court.[300]

In **Ireland** and the **United Kingdom**, Norwich Pharmacal-type actions have been brought against intermediaries in several cases. This rule permits a court to order a third party, who is not directly involved in litigation, to disclose documents in the third party's possession which relate to that litigation. If a court order is made, the third party is entitled to the reasonable costs of producing the material.[301]

In **Ireland** mainly copyright holders applied for court orders under the Norwich Pharmacal rule.[302] After carefully balancing the interests of right holders against the data privacy obligations of intermediaries[303], the court in *EMI v. Eircom* held that in the case of filesharing and where there was a *prima facie* case against the user, the balance lay in favour of disclosure. At the same time the court imposed safeguards, directing that the information disclosed could only be used to seek redress for the users' alleged copyright infringement

[295] NE6. – Court of The Hague, 05/01/2007, Stichting Brein vs KPN LJN number AZ5678, case number 276747/KG ZA 06-1417, disponible via www.rechtspraak.nl.
[296] See Part 1:D.IV.2.
[297] FR23. – TGI Paris, 27/02/2006, Alain Afflelou / Google, Free, http://www.legalis.net/breves-article.php3?id_article=1648.
[298] FR1. – TGI Paris, 20/04/2005, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres, FR2.. – TGI Paris, 13/06/2005, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres.
[299] FR3. – CA Paris, 24/11/2006, SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres.
[300] Art. 6 II LCEN reads as follows : « II. - Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.
Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.
L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa. (...) »
[301] Norwich Pharmacal Co and others v Customs & Excise Commissioners [1974] AC 133, [1973] 2 All ER 943, [1973] 3 WLR 164.
[302] Unreported, Smyth J., 12 July 2006. Outlined in "High Court rejects Ryanair bullying claim" *The Irish Times* 13 July 2006.
[303] [2005] IEHC 233.

activities and the identities of the alleged infringers could only be made public after the plaintiffs had started proceedings. In another case (*Maguire v. Gill*)[304] an order for third party discovery was made against an ISP requiring them to identify a user, but without considering whether or not the balance lay in favour of disclosure, and without explicitly ordering safeguards in respect of the use of this information.

Courts in the **UK** have applied the Norwich Pharmacal rule in cases relating to defamatory material on a discussion forum[305], and to the operator of a search engine (Google) who was ordered to disclose information about a recipient who had used the adwords service run by Google in order to make available a copyright-protected work.[306]

In the course of the implementation of **Art. 8 Enforcement Directive** (Directive 2004/48/EC[307]) member states already have introduced or will introduce claims for information that can be brought against intermediaries. For example the **German** Act on the Enhancement of the Enforcement of Intellectual Property Rights[308] is to introduce a special claim which according to the legislators intentions will also apply to internet intermediaries (§ 101 UrhG-Draft). Regulation 4 of Statutory Instrument 2006 No. 1028, the Intellectual Property (Enforcement, etc.) Regulations 2006, incorporates Art. 8 Directive 2004/48/EC (Enforcement Directive)[309] in **Scotland** and creates a new type of court order for disclosure of information about unlawful goods and services. With regard to **England, Wales and Northern Ireland** the explanatory note on Statutory Instrument 2006 No. 1028 holds that by reason of the Norwich Pharmacal rule[310] no provision is necessary to implement Art. 8 Directive 2004/48/EC.[311]

2. Data Protection

With regard to claims for information by private right holders against intermediaries, data protection has turned out to be one of the main issues. Just recently the Advocate General at the European Court of Justice[312] argued in the case of *Promusicae vs. Telefonica* that the

[304] Unreported, *ex tempore*, High Court, Hannah J., 5 October 2006.
[305] UK4. – High Court of Justice, Queen's Bench Division, 19/1/2001, Case No: HQ/0100536, (Totalise plc v Motley Fool Ltd and another), http://www.hrothgar.co.uk/YAWS/reps/totalise.htm.
[306] UK5. – Chancery Division, 17/5/2006, [2005] EWHC 3444 (Ch) – Grant v Google UK Ltd.
[307] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, OJ of 30.4.2004 157, 45.
[308] Gesetz zur Verbesserung der Durchsetzung von Rechten des geistigen Eigentums (Entwurf der Bundesregierung vom 24.01.2007), BR-Drucks. 64/07, available at: http://www.bundesrat.de/cln_051/SharedDocs/Drucksachen/2007/0001-0100/64-07,templateId=raw,property=publicationFile.pdf/64-07.pdf.
[309] Directive 2004/48/EC of the European Parliament and of the Council of 29.4.2004 on the enforcement of intellectual property rights, OJ 157/45 of 30.4.2004.
[310] Norwich Pharmacal v Customs and Excise Commissioners [1974] AC 133.
[311] Available at http://www.opsi.gov.uk/si/si2006/20061028.htm.
[312] Conclusions of the Advocate General Juliane Kokott of 18.7.2007, Case C-275/05, Productores de Música de Espana (Promusicae) v Telefonica de Espana SAU.

Enforcement Directive[313] does not set aside privacy directives such as the Directive on Protection of Telecommuncation Data 2002.[314]

a) *Promusicae vs. Telefonica*

Promusicae had identified a number of IP addresses that were at a specific point in time attributed to participants in filesharing. In order to prepare for legal action against these participants Promusicae demanded information on the names and addresses of the holders of the IP addresses at the relevant points in time from Telefonica. The Spanish court Juzgado de lo mercantil no. 5 in Madrid initially ordered Telefonica to disclose the requested information, but subsequently Telefonica relying on data protection laws, declared it could legally provide information only to public authorities for purposes of criminal investigation or in the interest of public safety or national security. The Spanish court referred the case to the European Court of Justice requesting a decision on whether community law permits or demands the communication of individual-related traffic data on the use of the internet to holders of intellectual property rights.

The Advocate General concluded that provisions in Community law on data protection in electronic communications permit the communication of individual-related traffic data only to the competent public authorities, but not a direct communication to the holders of copyrights who intend to take civil legal action. Accordingly, a provision prohibiting the communication of traffic data for purposes of civil legal action complies with Community law. The Advocate General reasoned that the information on which users were attributed a specific IP-address at a specific point in time constitutes "personal data" in terms of Art. 2 (a) of Directive 95/46/EC[315], i. e. information relating to an identified or identifiable natural person. By means of this data the actions undertaken using the respective IP-address are connected to the holder of the telephone line. The communication of this data constitutes "processing" in terms of Art. 2 (b) Directive 95/46 EC. At least the temporarily attributed IP-addresses of users are traffic data in terms of Art. 2 (a) Directive 2002/58/EC, i. e. data processed for the purpose of the conveyance of a communication on an electronic communications network.

If the European Court of Justice follows this line of argument, providers will not be entitled to disclose information about their users. The conflict between enforcement of copyrights, data privacy, and the intermediary role of providers lies at the core of most of the cases and decisions.

[313] Directive 2004/48/EC of the European Parliament and of the Council of 29.4.2004 on the enforcement of intellectual property rights, OJ 157/45 of 30.4.2004.
[314] Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201/37 of 31.7.2002.
[315] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31 of 23.11.1995.

b) Data Protection Issues in National Case Law

Courts (or administrative agencies) in some member states explicitly refer to privacy statutes when they refuse to acknowledge private claims against providers to disclose data about their users (identity, traffic etc.), like in **Belgium** (as the Belgian Data protection Commission has declared that rights holders are not allowed to deal with IP addresses).

In **France**, copyright associations have also tried to retrieve the data of users of P2P-systems. Art. 9 § 4 LCEN permits 'sociétés de gestion collective', if they get CNIL (Commission Nationale Informatique et Libertés) agreement, to process personal data in order to protect copyrights. In four recent **French** cases concerning IP addresses,[316] these were held not to be identification data, following the advice from the CNIL, as they cannot be used for the purpose of tracking users. According to the judges, they are only linked with the computer and not with the persons. Very recently, the TGI of Paris in the Techland case declared that even if a court ordered access providers to disclose IP addresses to the copyright holder, the latter was required to inform the CNIL that he was doing so. The lawyer of the copyright holder (who is French and in France) did not inform the CNIL. Therefore, the TGI broke the ordinance given to the Access providers to collect and disclose IP's.[317] In 2005, the CNIL refused agreement to several companies, judging that the extent of data processing was disproportionate to the aim of patrolling P2P networks. The Conseil d'Etat[318] recently overruled the CNIL decision, declaring that there was no disproportion. The outcome relating to data processing is still therefore unclear.

In **Italian** cases concerning copyright infringements via P2P-networks a record company sued several access providers, under article 156 bis of the Copyright Act, demanding the names and addresses of the peer-to-peer systems users. After the Court of Rome in a first case had already granted an injunction ordering intermediaries to reveal the addresses of their customers, identified by logs,[319] the court in a second case apparently changed its opinion and dismissed the claim for disclosure of information.[320] In its ruling the court largely relied on the Data Protection Commissioner's opinion who had argued that the disclosure of users' logs and personal data (such as e-mails and addresses) represented an invasion of privacy. It is likely that the Court of Appeal will overrule the Court of Rome's first decision by following this line of reasoning.

In **German** cases related to host providers, the courts have up to now rejected claims for information referring inter alia to data protection provisions that did not give providers the

[316] TGI Montauban, 09/03/2007, *Ministère public, La société des Producteurs Phonographiques c/ Madame M. L .* ; CA Paris, 27/04/2007, *Monsieur G. c/ Ministère public, Société civile des Producteurs Phonographiques* ; CA Paris, 15/05/2007, *Monsieur H. S. c/ Ministère public, Société civile des Producteurs Phonographiques*

[317] Techland case, unpublished.

[318] Conseil d'Etat Section du contentieux 23 mai 2007, Sacem et autres / Cnil.

[319] IT8. – Tribunale di Roma, Sezione IX civile (IP specialized section), 9th February 2007 – Peppermint Jam Records v. Telecom Italia.

[320] IT9. – Tribunale di Roma, Sezione IX civile (IP specialized section), 14th July 2007 – Peppermint Jam Records v. Telecom Italia; Tribunale di Roma, Sezione IX civile (IP specialized section), 14th July 2007 – Peppermint Jam Records v. Wind Telecomunicazioni spa.

right to disclose data to holders of intellectual property rights.[321] The new German TMG allows providers to disclose user data to holders of intellectual property rights (§ 14 (2) TMG); However, it is still unclear whether the new provision in § 14 (2) TMG also covers access providers[322]; for that reason, Parliament plans to adopt a rule similar to the TMG in the new Telecommunication Act (see § 113b TKG-Draft) which is to incorporate Directive 2006/24/EC[323]. This regulation could be considered also as a reaction to the prevailing court decisions. Nevertheless, it is not quite clear whether these reforms will be in line with European directives in view of the latest Promusicae case currently before the European Court of Justice.[324]

According to the decision of an **Austrian** court a request for information on holders of dynamic IP addresses only referred to customer data and did not require access to traffic data protected by the principle of privacy of communications and may therefore only be accessed after judicial authorisation provided the conditions of § 149a StPO have been met.[325] In this context the court followed the reasoning of the Supreme Court of Justice in its decision of 26.7.2005.[326]

Under **Irish** data privacy laws, intermediaries are not entitled to share customer information with anyone except in cases where a court order has been issued against them. In *EMI v. Eircom*[327] a *Norwich Pharmacal-type* action was brought by record companies in order to compel ISPs to identify users accused of file-sharing. The court accepted that the ISPs acted properly in not volunteering this information and that they owed duties of confidentiality and data privacy to their users.

In a case involving defamatory material on a discussion forum, a court in the **UK** stated that there was no reason under the Data Protection Act 1998 for providers to withhold identity data.[328]

V. Obligations to Retain Data

Closely connected to obligations to reveal information at the request of public authorities are obligations to keep and store data about user`s identities and traffic data:

In **France** Art. 6-II LCEN and Articles L.34-1 and L.34-1-1 of the "Code des Postes et des Communications Electroniques" **compel providers to store connection data**. These articles diverge slightly and it is still difficult to ascertain what exactly the access providers are

[321] GE11. – KG Berlin, 25.9.2006, 10 U 262/05, MMR 2007, 116, see also Part 1:D.IV.2.
[322] See *Spindler*, CR 2007, 239 (243).
[323] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105/54 of 13.4.2006.
[324] See Conclusions of the Advocate General Juliane Kokott of 18.7.2007, Case C-275/05, Productores de Música de Espana (Promusicae) v Telefonica de Espana SAU.
[325] AU2. – HG Wien, 21/6/2006, 18 Cg 67/05, http://www.internet4jurists.at/entscheidungen/hg67_05w.pdf.
[326] AU1. – OGH, 26/7/2005, 11 Os 57/05z, 11 Os 58/05x, 11 Os 59/05v, http://www.internet4jurists.at/entscheidungen/ogh11_57_05z.pdf.
[327] [2005] IEHC 233.
[328] UK4. – High Court of Justice, Queen's Bench Division, 19/1/2001, Case No: HQ/0100536, (Totalise plc v Motley Fool Ltd and another**)** http://www.hrothgar.co.uk/YAWS/reps/totalise.htm.

supposed to do. First, in the Tiscali case, a host provider was found negligent for not checking identification data.[329] In the Paribas ruling the Cour d'appel de Paris[330] interpreted the law differently. The judge explained that even if Art. 6-II LCEN does compel providers to keep identification data, it does not compel them to verify them. In a case involving Ebay (Grenoble 2007[331]), the judge endorsed this interpretation. The TGI of Paris stated that, following the ECD, the search engines have no obligation to keep details of their users[332] as they have no clients as such and do not therefore need to keep tracks of who searched for what in order to offer the service. Consequently, the judge declared that identification data questions do not apply to search engines.

As already described above, the **Italian** act against child pornography requires intermediaries to keep information on companies and subjects that distribute, disseminate or trade child pornographic materials for at least 45 days from communicating to the National Centre.[333]

In the famous **Dutch** case of *Stokke BV vs Marktplaats BV*[334], the Court decided that details of clients did not have to be analyzed and kept by a host provider; the judges deemed such a obligation to be unreasonable in view of the expenses involved in collecting and keeping data, set against the potential usefulness of the data collected. However, one should note that the court referred in its judgement to specific circumstances of the case such as the ease with which the right-holder could obtain data directly by answering to infringing offers and thus getting details of the advertisers (infringing e.g. trademarks).

Other member states, such as **Ireland**, have introduced specific data retention obligations for ISPs,[335] such as Part 5 of the Irish Criminal Justice (Terrorist Offences) Act 2005 in respect of traffic and location data for fixed line and mobile telephony, which requires access service providers to store such data for three years. Whereas such obligations do not require ISPs directly to report infringements to authorities, they are bound to assist state authorities by disclosing relevant information.

---

[329] FR7. – TGI Paris, 16/02/2005, *Dargaud Lombard, Lucky Comics/Tiscali Média*.http://www.legalis.net/breves-article.php3?id_article=1420, FR8. – CA Paris, 07/06/2006, *Dargaud Lombard, Lucky Comics/Tiscali Média,* http://www.legalis.net/jurisprudence-decision.php3?id_article=1638#

[330] FR5. - CAParis, 04/02/2005, *SA BNP Paribas c/ Société World Press Online*.http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=867 http://www.foruminternet.org/telechargement/documents/ca-par20050204.pdf

[331] FR14. – TI Grenoble, 01/02/2007, Contoz / EBay International, http://www.droit-technologie.org/upload/jurisprudence/doc/228-1.pdf

[332] FR23. –TGIParis, 27/02/2006, http://www.legalis.net/breves-article.php3?id_article=1648.

[333] Article 14 of the Law No. 269 of 1998 "Exploitation of child prostitution, child pornography and child sex tourism as new forms of slavery".

[334] NE15. – District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV,LJN number AW6288, case number 106031/HA ZA 05-211, available via www.rechtspraak.nl; NE16. – District Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, available via www.rechtspraak.nl.

[335]This report can not deal with all data retention specific obligations or provisions as these are closely related to the data privacy directives (telecommunication directives) which are not the subject of this report.

E. Specific Services

I. Auction Platforms

Auction Platforms, such as ebay, are one of the leading e-commerce applications and have been at the centre of some important court rulings in member states:

1. Qualification as Host Providers

Auction platforms are qualified by the **German** Federal Court of Justice as host providers as they do not act on their own by storing offers of third parties. This is the case even if the auction operator benefits from successful auctions by charging the supplier a commission.[336] The **Austrian** Supreme Court of Justice has followed the same approach. The court held that a host provider is not only the operator of a server where content is stored, but so is any other service provider who is in a contractual relationship with the operator of the server and who (on his behalf) offers his recipients/customers storage opportunities - for example operators of online forums or **online auction platform**s.[337]

However, this clear-cut definition and approach, which is largely undisputed in Germany, is contrasted by the approach of courts in other member states. **Dutch** courts have left open the issue of whether a marketplace forum can be qualified as a host provider.[338] **French** courts[339] have ruled - in litigation concerning the contractual liability of ebay[340] - that auction platforms have to be declared to be a kind of technical intermediary; however, the classification of an auction platform (host provider? Content provider?) remains unclear. The courts –primarily concerned about the contractual liability of an auction platform operator towards the participants in an auction - state that the auction platform provider is not responsible for the execution of the contract agreed between the seller and the bidder. The French decisions also stated that the auction platform provider has a data retention obligation, though it is not expected to check whether the data provided by customers are correct.

It is very important to remind that jurisprudence concerning auction platforms in **France** is still changing and that no precise qualification was given by Courts. A ruling between Ebay

[336] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 – Internetversteigerung I; GE13. – BGH, 19.4.2007, I ZR 35/04 – Internetversteigerung II. Both decisions assess the applicability of § 10 TMG/§ 11 TDG dealing with hosting; *Spindler*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, 2005, Kap. 6 Rz. 5 ff..

[337] OGH, 11.12.2003, 6 Ob 218/03g (the decision concerned the liability of a content provider).

[338] NE15. – District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031/HA ZA 05-211, available via www.rechtspraak.nl; see also NE16. – Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, available via www.rechtspraak.nl - which, however, does not deal with the duty of care principle.

[339] FR11. – TI Saint Jean de Maurienne, 06/08/2003, Bruno Alexrad c/ Ebay France SA, www.droit-technologie.org/redirect.asp?type=jurisprudence&juris_id=160&url=juirsprudence/TI_StJeanMaurienne_060803.pdf, http://www.droit-technologie.org/upload/jurisprudence/doc/159-1.pdf; FR12. – Prox Pau, 26/02/2004, Monsieur Rick D. c/ eBay, http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=765, www.forumInternet.org/telechargement/documents/documents/jprox-pau26022004.pdf ; FR14. -TI Grenoble, 01/02/2007, Contoz / EBay International, http://www.droit-technologie.org/upload/jurisprudence/doc/228-1.pdf.

[340] Ebay was accused of not having supervised its platform and thus contributed to a damage a buyer suffered from escroquerie.

and Louis Vuitton is pending. The TGI of Paris, if called upon, will certainly precise the qualification of the auction platform.

In **Swedish** law the concept "electronic bulletin board" is understood to have the same meaning as "hosting" and an internet auction platform is regarded as an interactive bulletin board under the Act on Responsibility for Electronic Bulletin Boards[341]. Swedish auction platforms (ebay), however, have not yet complained about any action by the authorities (like injunctions or fines etc.).

2. Injunctions against Providers of Auction Platforms

In contrast to the vast majority of member states, **Germany** has generated a substantial number of cases on auction platforms. Indeed, these cases are the leading judgments on host providers and injunctions, and thus generally influence the interpretation of the ECD's implementing legislation in Germany (the TMG).

Court cases have concentrated (again) on injunctions, stating that the liability exemptions of the TMG are not applicable. Hence, courts apply general provisions of civil law on responsibility concerning the so-called "Störerhaftung" (accessory liability).[342] Only recently, the Federal Court of Justice extended the concept of accessory liability to unlawful competition concerning infringements of protection of minors committed by suppliers on an auction platform.[343] The Court held that the operator of the auction platform was, in principle, obliged to act upon notice of illegal practices. The case was referred back to the Court of Appeal for further consideration of the scope of the obligation to examine, and the possibilities of using filter software and other technical means to identify content harmful to minors.

A **Dutch** court explicitly followed the reasoning of the German High Federal Court by acknowledging injunctions against a marketplace provider and stating that a host provider is obliged to prevent and terminate infringements.

In **France**, one court held that the sale of copyrighted video games on an internet store (and which were obviously too cheap in comparison to normal store prices) constitutes a manifest infringement, and thus ordered the provider to stop access to all such offers. However, the reasons the court gave are very short.[344]

[341] Available at: http://www.sweden.gov.se/content/1/c6/02/61/42/43e3b9eb.pdf.
[342] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 (671) – Internetversteigerung I; GE13. – BGH, 19.4.2007, I ZR 35/04 – Internetversteigerung II; see also GE 27. – BGH of 1.4.2004, I ZR 317/01, GRUR 2004, 693 (695) – Schöner Wetten (regarding hyperlinks); for more details concerning the German concept of accessory liability which is rather different to the situation in other member states see the German Country Report.
[343] GE14. – BGH, 12.7.2007, I ZR 18/04. For the initial decision of the court of appeal OLG Brandenburg, 13.6.2006, 6 U 114/05, MMR 2006, 617.
[344] FR13. – Comm Paris, 17/10/2006, *Konami c/ Babelstore,* www.droit-technologie.org/jurisprudence/details.asp?id=224.

II. Information Location Tools

The legal situation concerning information location tools, in particular hyperlinks and search engines,[345] is inconsistent across member states. As the ECD deliberately refrained from regulating hyperlinks and search engines, member states were able to design their own liability regimes for these information location tools. However, only some member states introduced specific norms which deal with liability of hyperlinks and of search engines, such as Austria, Hungary, Portugal, and Spain.

Moreover, it seems sometimes difficult for courts to distinguish clearly between a direct infringement of (e.g.) intellectual property rights by a search engine (or hyperlink) and those infringements which consist of contributing to third party contraventions.

Finally, there is no clear-cut definition of hyperlinks or search engines. In order to distinguish between the different legal approaches in member states it is necessary to take into account the various functions of search engines and hyperlinks:

- Search engines are mostly those services which automatically search the internet for content which has been characterized by a few "search words" determined by the user. As a result the search engine offers the user a spectrum of hyperlinks which may lead to the desired content. Thus, their way of working resembles a technical tool that enhances access to content by means of automatic referencing to the desired content. However, it has to be taken into account that search engines can concentrate on searching specific contents like pictures, music or other digital content. Moreover, they may be designed for specific purposes such as searching the Usenet for music in MP3 format.
- In contrast, a hyperlink is set manually, thus indicating that an individual is consciously selecting content to which the hyperlink addresses users. Hence, setting a hyperlink implies necessarily the actual knowledge of the content to which the hyperlink directs the user. However, it does not imply that the person setting the hyperlink is aware of any changes in the content which are made after the hyperlink has been set.
- Finally, there are hybrid forms between search engines and hyperlinks, like web sites containing hyperlinks which previously have been produced by a search engine. Thus, the hyperlinks are not specifically used by one user (who has typed in the relevant search words) rather than by a community. In other terms, search results are published to a large community rather than only to one individual searching user.

There are several notions which are more or less commonly used across member states such as:

- Commercial links: Although these hyperlinks are created by a search engine they differ from "natural links" as they are not only a result of the search process but rather a combination of the search and previously bought "advertising words" by a client of

[345] Note that in Portugal the notion of « content aggregator » obviously refers to hyperlinks and search engines as these are deemed to aggregate « content » by referencing third party content.

the search engine. Hence, every time a user is looking for content which is characterized by typical words, commercial links will pop up as well as the "normal" (or "natural") hyperlinks being provided by the search engine. "Commercial links" is a system used in particular by Google in order to generate advertising income. Clients are offered a word (of their own choice) that will be associated with the results of a defined request. Thus, anyone can pay for and choose his own commercial link as the system operates automatically without checking in advance whether the buyer of the word is really entitled to use it.

- Deep links: These links refer the user directly to content, bypassing the root home page and therefore often bypassing advertisements on the root page.

1. Distinction between own infringements and contribution to infringement of other persons

First, the distinction between the infringements of a provider of information location tools (search engines and hyperlinks) and mere contribution to third party infringements is crucial, in particular for copyright issues:

In one famous Belgian case (*Copiepress v. Google*), the court[346] held that the services "Google News" and "Cache Google" infringed copyright and ancillary rights. The search engine's behaviour was found to be unlawful on the grounds that it constituted a direct violation of copyright by the publication of content without the authors' prior consent, due to the fact that Google obviously copied the content for more than a short period. Hence, it was not a case of liability for third party infringements rather than for a direct infringement by Google. Consequently, application of the Belgian e-commerce law was not relevant – the case could be dealt with under copyright law. Prior decisions[347] had required the search engine to remove from its websites all Belgian press links, articles, photos and graphic representations. Google also had to publish the judgement on the homepage of google.be and Google News.

Moreover, closely related to deep linking are cases concerning search engines that contain direct references to web content. In some member states, like **Denmark**, the courts previously construed such search engine activities as copyright infringement for which liability applies.[348] However, since 2006, Danish courts have held this sort of automatic referencing by search engines to be legal.[349]

Dutch courts are ambiguous about deep linking to databases:[350] The Supreme Court held that deep links (created by a search engine) constitute an infringement of the rights and that

[346] BE17. – Tribunal de première instance de Bruxelles, 13.2.2007, www.droit.be, (CopiePresse c. Google).
[347] BE15. – Tribunal de première instance de Bruxelles (cessation), 5.9.2006, www.droit.be, n° 2006/9099/A, (CopiePresse c. Google)
BE16. – Tribunal de première instance de Bruxelles (opposition), 22.9.2006, www.droit.be, (CopiePresse c. Google).
[348] DE2. – Copenhagen Bailiff's Court, 05/07/2002, DNPA vs Newsbooster, available on the CD.
[349] DE3. – Maritime and Commercial Court of Copenhagen, 24/02/2006, Danish real estate chain home vs Ofir, available on the CD.
[350] Country Report Netherlands Case NE 19 – 21: Rechtbank 's-Gravenhage, 12/09/2000, NVM vs De telegraaf, LJNnumber AA8588, case number KG 00/949, available via www.rechtspraak.nl . Gerechtshof 's-Gravenhage, 21/12/2000, NVM vs De telegraaf, LJNnumber AB0450, case number 00/1053, available via

therefore a search engine using them is liable – in contrast to other courts in the same case. However, more recently, the Court of Arnhem[351] confirmed the concept of a search engine as only building references to other contents from the Internet.

2. Search Engine Operators

a) Specific National Regulations Concerning Search Engine Operators

The **Austrian** legislator introduced a special liability exemption for search engines (and other information location tools) largely corresponding to § 13 ECG (which refers to access providers). The explanatory memorandum as given by the parliament stresses the fundamental importance of search engines for quick and efficient use of the internet. However, there is no official definition of "search engine" in Austrian law. According to the explanatory memorandum the lines between the different types of search services are fluid. However, injunctions are left untouched by this liability exemption (as clarified by § 19 (1) ECG).

In a similar way, **Hungary** has provided for a specific liability exemption for information location tools. According to § 2 ld) ECSA, search engine operators offer resources that facilitate the finding of information for users. However, in contrast to Austrian law, Hungary qualifies them as host providers and applies Art. 14 ECD in an analogous way (§ 11 ECSA), since search engines do no more than rank the information made available.

The same approach as in Hungary is followed by **Spain**, which implemented the ECD by law n° 34/2002 of July 11th, 2002. Article 17 of this law establishes a liability exemption for hyperlinks and search engine providers which adopts the same liability rules as for host providers, that is, effective knowledge given by a competent body. However, no Spanish judge has yet handed down a decision regarding search engines.

Portugal also has specific liability provision in its implementing law for intermediary service providers associated with content by means of search engines, hyperlinks or similar procedures (like directories). As a general rule, the intermediary is subject to the same liability rules as host providers. Two Portuguese administrative resolutions (provisional settlements of disputes) have been issued against host providers and intermediary service providers associated with content by means of search engines.[352]

b) Member States applying general principles of law

In **France**, there is no specific regime for search engines, even though French courts have sometimes qualified a search engine as a host provider.[353] "Natural results" are the core

www.rechtspraak.nl. Hoge Raad, 22/03/2002, NVM vs De telegraaf, LJNnumber AD9138, case number C01/070HR, disponible via www.rechtspraak.nl .

[351] Country Report Netherlands Case NE 24 – 25,Court of Arnhem, 16/03/2006, NVM vs ZAH, LJN number AV5236, case number 136002, available via www.rechtspraak.nl; Court of Appeal Arnhem, 04/07/2006, NVM vs ZAH, LJN number AY0089, case number A6/416, available via www.rechtspraak.nl .

[352] Administrative resolution from the National Authority of Communications (ANACOM) – 18.05.04 – Case Nokia Portugal v. Verza Facility Management, Google and others; Administrative resolution from the General Inspection of Cultural Activities – 2005.

[353] FR9. – Comm Lille, 01/06/2006, STE Espace Unicis c/ SA Meetic, SARL Google France www.juriscom.net/documents/tclille20060601.pdf.

elements of search engines: browsing the internet with computers and indexing keywords automatically. As far as "natural results" are concerned, search engines have not been held liable.[354] One judge[355], in reference to LCEN, explicitly referred to the "creation" of hyperlinks in a search engine as an automatic and technical procedure; therefore the judge explicitly declared that a monitoring obligation would not be reasonable. Nevertheless, when illicit content is notified search engine operators are obliged to take action promptly in order to avoid liability.[356] Concerning illicit content like revisionism and racism, the French courts have stated that search engines have to filter the contents of their automated indexes.[357]

Germany has not adopted specific legislation on liability of search engines. The legislator deliberately refrained from regulating hyperlinks and search engines. The German Federal Court of Justice has affirmed the view that the German implementation act cannot be applied analogously to hyperlinks[358] and search engines, even though some legal scholars (in a minority) still disagree in spite of the clear wording in parliamentary documents relating to its legislative passage. Hence, following the "*Schöner Wetten*" decision by the Federal Court of Justice, courts in general deny the applicability of the liability exemptions of §§ 8 to 10 TMG for search engine providers.[359]

However, injunctions continue to play a dominant role in practice, although the German Federal Court of Justice has not yet ruled on this issue. Lower courts usually refer to the "*Internetversteigerung I*"[360] decisions of the Federal Court of Justice (concerning auction platforms) and "*Schöner Wetten*"[361] (concerning hyperlinks) and apply these principles to cases involving search engines.[362] Most courts have held that in principle search engine providers are not subject to a monitoring obligation so long as the operator had not been given notice of an infringement (especially by way of a warning letter). They have pointed to the socially desirable function which search engines perform.[363] However, most of the decisions concern the liability of search engine operators for "*adwords*".

---

[354] FR 36. – CA Paris, 15/05/2002, Société Altavista c/ Société Matelsom et Société Literitel, 15/05/2002, www.forumInternet.org/telechargement/documents/ca-par20020515.pdf, FR16. – TGI Paris, 31/07/2000, www.juriscom.net/txt/jurisfr/cti/tgiparis20000731.pdf .

[355] FR37. – TGI Paris, référé, 12 mai 2003, Lorie c/ M. G.S. et SA Wanadoo Portails www.juriscom.net/documents/tgiparis20030512.pdf .

[356] FR23. – TGI Paris, 27/02/2006, Alain Afflelou / Google, Free http://www.legalis.net/breves-article.php3?id_article=1648,available on the CD.

[357] FR33. – TGI Paris, 22/05/2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France , available on the CD; FR34. – TGI Paris, 20/11/2000, UEJF et Licra c/ Yahoo! Inc. et Yahoo France www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf ; FR12. – Prox Pau, 26/02/2004, *Monsieur Rick D. c/ eBay* www.juriscom.net/txt/jurisfr/cti/tgiparis20020226.pdf ; FR35. – TGI Paris, 11/02/2003, UEJF et Licra c/ Yahoo! Inc. et Yahoo France www.forumInternet.org/telechargement/documents/tgi-par20030211.pdf .

[358] GE27. – BGH, 1.4.2004, I ZR 317/01, MMR 2004, 529 - Schöner Wetten.

[359] KG,10.2.2006, 9 U 55/05, MMR 2006, 393 (395); GE21. – LG Berlin, 22.2.2005, 27 O45/05, MMR 2005, 324; GE19. – LG Berlin, 9.9.2004, 27 O 585/04, MMR 2004, 786; GE24. – LG Hamburg, 16.9.2004, 315 O 755/03, MMR 2005, 480.

[360] GE12. – BGH, 11.3.2004, I ZR 304/01, MMR 2004, 668 (671) – Internetversteigerung I.

[361] GE27. – BGH, 1.4.2004, I ZR 317/01, GRUR 2004, 693 - Schöner Wetten.

[362] GE19. – LG Berlin, 9.9.2004, 27 O 585/04, MMR 2005, 786; LG Hamburg, 28.4.2006, 324 O 993/05 (not officially published), see http://www.suchmaschinen-und-recht.de/urteile/Landgericht-Hamburg-20060428.html.

[363] GE18. – OLG Hamburg, 20/2/2007, 7 U 126/06, http://www.suchmaschinen-und-recht.de/urteile/Oberlandesgericht-Hamburg-20070220.html; KG, Urt. v. 10.2.2006 – 9 U 105/05, NJW-RR

In contrast to France and Germany, **Italy** has only reported one criminal case (Postal Police) involving a search engine. The case concerned the "publication" of a video by a search engine showing a group of four Italian teenagers bullying a 17-year-old disabled boy in a classroom. The search engine had deleted the movie as soon as it was informed about it[364]. The Postal Police clearly treated the search engine as a content provider; Italian legal scholars, however, describe search engines as host providers in the light of Legislative Decree No. 70.[365]

In the **Netherlands**, the courts have regarded search engines as an internet intermediary that only collects and builds references to other internet content – however this position was established before the implementation of the ECD in Dutch law.[366] More recently (in contrast) the court in *TechnoDesign v Stichting Brein*[367] denied the applicability of the liability exemption because (according to the first instance judgment) the owner of the search engine knew it was referring to illicit content, in particular that the bulk of his clients was looking for copyrighted material, and because (in the Court of Appeal) a search engine is not an internet intermediary. Thus, the search engine operator was held liable for referencing to copyright infringing MP3 files. This Court's opinion has, however, been widely criticized.[368]

In **UK**, the DTI has recently considered whether to explicitly extend the liability limitations in Articles 12 to 14 ECD to hyperlinkers, location tool services and content aggregation services, but has concluded that there is currently no substantial evidence to support the case for an extension.[369] However, it also noted in the DTI report that the legal situation as regards the need for an exemption on liability is less clear in some other member states (i.e. France and Germany).

In most member states without specific regulations decisions are made on the basis of academic theory on how to treat or describe search engines and hyperlinks. In the **Czech Republic**, for example, search engines cannot be responsible for the content of a hyperlink if they are not aware of the unlawfulness of the content (and vice-versa).[370] The same applies to **Poland** where the legal literature defines a "search engine" as software which

2006, 1481; GE21. – LG Berlin, 22.2.2005, 27 O 45/05, MMR 2005, 324 (325); GE19. – LG Berlin, 9.9.2004, 27 O 585/04, MMR 2005, 786; GE3. – LG Hamburg, 28.4.2006, 324 O 993/05 (not officially published), http://www.suchmaschinen-und-recht.de/urteile/Landgericht-Hamburg-20060428.html.

[364] There was no official decision, only a police seizure.

[365] G.M. Riccio, La responsabilità civile degli internet providers, Giappichelli, Torino, 2002, 220-221; P. Sammarco, Il motore di ricerca, nuovo bene della società dell'informazione: funzionamento, responsabilità e tutela della persona, in Diritto dell'informazione e dell'informatica, 2006, 621

[366] NE18. – Rechtbank 's-Gravenhage, 14/01/2000, KPN vs XSO, LJNnumber: AA4712, case number: KG 99/1429, available via www.rechtspraak.nl.

[367] NE22. –Court of Haarlem, 12/05/2004, Technodesign vs Stichting Brein, LJN number AO9318, case number 85489/HA ZA 02-992, available via www.rechtspraak.nl.
NE23. – Gerechtshof Amsterdam, 15/06/2006, Technodesign vs Stichting Brein, LJN number AX7579, case number 1157/04, available via www.rechtspraak.nl.

[368] Dutch lawyers engaged in several companies fight for a legal frame for hyperlinks and search engines. Most of the stakeholders acting for Intermediaries interests approve and want an equal treatment for search engines comparably to the host providers' regime.

[369] See http://www.dti.gov.uk/consultations/page13985.html.

[370] Cermak X, Internet and Copyright, Linde Praha, 2001.

helps internet users in searching for specific information on the internet by providing a list of hyperlinks to websites which might contain the requested information.[371]

c) Sponsored Links (Commercial Links; adwords)

The bulk of cases do not concern "natural links" (or automatic generated links referring to contents indexed by the search engine) but rather to "commercial links" or "adwords".[372]

Most of the cases concerning "commercial links" have been reported in **France**:[373] There, most courts have refused to classify the search engine and its service as a technical intermediary[374] and, in particular, neither as a host provider under the ECD (the French implementation Act, the LCEN)[375] nor as an access provider.[376] There are a few notable exceptions to this approach, such as that taken by the Tribunal de Commerce Lille and by the TGI of Strasbourg which qualified Google as host provider for adwords.[377] The basic reasoning applied by the court was that Google sells "adwords" and thus, the search engines does not act as a mere technical intermediary. Rather, it takes an active role in selling the relevant search words for "commercial links" and generates revenue by these activities.[378] Most French courts have held – on grounds of trademark law – that a search engine provider has to analyse the purchasing request for an adword before selling commercial links, in order to prevent copyright infringements. Technical reasons addressing the problems of automatically checking the legitimacy of the use of adwords by clients have not been acknowledged by French courts.[379] Moreover, search engines are liable for infringements

[371] Beata Gadek, Wprowadzenie w blad wyszukiwarek internetowych w swietle ustawy o zwalczaniu nieuczciwej konkurencji, Przeglad Prawa Handlowego, nr 8/2005, S. 47.

[372]The terminologiy differs widely across member states ; however « commercial link » (for France) and « adwords » (for Germany) seem to be the most commonly used notions.

[373] For a more detailled analysis of the many French cases (FR17 and others) see Country Report France E.1.

[374] See in particular: FR25, 26 - Court d`Appel Paris, 28/06/2006, SARL Google, Sté Google Inc c/ SA Louis Vuitton Malletier, www.juriscom.net/documents/caparis20060628.pdf; FR29 CA Versailles 02/11/2006, Sarl Overture et Sté Overture Services Inc c/ SA Accor, www.juriscom.net/documents/caversailles20061102.pdf ; FR13 - TGI Nanterre, 13/10/2003, www.juriscom.net/documents/tginantere20031013.pdf ; FR14 - TGI Nanterre, 14/12/2004, www.forumInternet.org/telechargement/documents/tgi-nan20041214.pdf ; FR18 - TGI Nanterre, 16/12/2004, www.juriscom.net/documents/tginanterre20041216.pdf ; FR21. – TGI Paris, 24/06/2005, AMEN c/ Espace 2001 et Google France , www.juriscom.net/documents/tgiparis20050624.pdf; FR24. – TGI Nanterre, 02/03/2006, Hôtels Méridien / Google France http://www.legalis.net/breves-article.php3?id_article=1599.

[375] See in particular: FR20. – CA Versailles, 10/03/2005, Google c/ Viaticum, Luteciel, http://www.juriscom.net/documents/caversailles20050310.pdf

[376] FR 23 – TGI Paris, 27/02/2006, Alain Afflelou / Google, Free, http://www.legalis.net/breves-article.php3?id_article=1648.

[377] FR9 – CommLille, 01/06/2006, www.juriscom.net/documents/tclille20060601.pdf; affirmed in Case FR10 – TGI Strasbourg, 20/07/2007, Atrya/Google France et autres, http://www.legalis.net/jurisprudence-decision.php3?id_article=1995.

[378] Clearly stated in FR18 – TGI Nanterre, 14/12/2004, CNRRH, Pierre Alexis T. c/ Google France et autres, http://www.foruminternet.org/telechargement/documents/tgi-nan20041214.pdf; also in FR20 - CA Versailles, 10/03/2005, Google c/ Viaticum, Luteciel, http://www.juriscom.net/documents/caversailles20050310.pdf.

[379] FR20. – CA Versailles, 10/03/2005, *Google c/ Viaticum, Luteciel* www.juriscom.net/documents/caversailles20050310.pdf; FR28. – TGI Paris, 11/10/2006, Citadines / Google Inc, Google France.http://www.legalis.net/jurisprudence-decision.php3?id_article=1765
TGI Paris, 31/10/2006, unpublished; ,FR3. – CA Paris, 24/11/2006, SA Tiscali, *Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres*, www.forumInternet.org/telechargement/documents/tcom-par20061124.pdf.

according to tort law as well.[380] In one judgment, the Tribunal de Grande Instance of Paris decided to hold a search engine liable for both tort and copyright infringements.[381] Hence, search engines have to operate preventive checks on their commercial link systems with regard to the kind of commercial links their clients want to buy and see whether such choices would infringe copyright and/or trademarks.[382] This, however, causes great technical difficulties to search engines since automatic systems – at least at present – are not able to automatically check on the complex legal aspects of trademarks or copyrights (a fact explicitly acknowledged by the Tribunal de Commerce Lille and by the TGI of Strasbourg).[383]

By contrast, **Austrian** and **German** courts have mainly rejected the notion of liability of search engine providers for adwords/commercial links. However, the distinction between liability for one's own activities (i.e. offering certain words which can be bought by clients) and for third party activities is a very subtle one: In Austria, the Supreme Court had to decide on the liability of a search engines operator for "adwords".[384] Here the focus lied upon its liability as a "helper" which in turn would have required that it had deliberately promoted the activities of the actual wrongdoer. Therefore, it must be proved that the helper has contributed to or facilitated the wrongdoer's action. Following the reasoning of prior decisions relating to the liability of intermediaries, the court held that a search engine operator may only be liable for alleged infringements committed by customers by way of keyword-advertising if the infringements would have been obvious to a non-lawyer without further investigation.[385] Without prior warning, the search engine operator was not obliged to examine the keywords used by advertising customers for possible infringements of trademark or competition law. The search engine operator would be subject to an obligation to act only in the event that the infringement would have been obvious to a non-lawyer. Only in the case of an obvious infringement could a deliberate promotion of the wrongdoer's activities by the search engine operator be found.

Most **German** courts have also held that search engine providers are not, in principle, subject to an obligation to examine, as long as the operator did not obtain notice of an infringement (especially by way of a warning letter), due to only marginal obligations to monitor in advance general content, and the socially desirable function performed by search engines.[386]

---

[380] FR22. – TGI Paris, 08/12/2005, Kertel c/ Google France, Google Inc. et Cartephone www.juriscom.net/documents/tgiparis20051208-2.pdf; FR27. – ,TGI Paris, 12/07/2006, GIFAM et autres c/ Google France www.juriscom.net/documents/tgiparis20060712.pdf; FR31. – TGI Paris, 13/02/2007, Laurent C. / Google France.

[381] TGI Nanterre, 16/11/2006, www.forumInternet.org/telechargement/documents.tgi-nan20061116.pdf.

[382] FR32..– CAVersailles, 10/03/2005, www.juriscom.net/documents/caversailles20050310.pdf

[383] FR9. – Comm Lille, 01/06/2006, *STE Espace Unicis c/ SA Meetic, SARL Google France,* www.juriscom.net/documents/tclille20060601.pdf.

[384] AU9. – OGH, 19/12/2005, 4 Ob 194/05s, http://www.internet4jurists.at/entscheidungen/ogh4_194_05s.htm.

[385] AU6. – OGH, 6/7/2004, 4 Ob 66/04s, http://www.internet4jurists.at/entscheidungen/ogh4_66_04s.htm (megasex.at); AU7. – OGH, 24/5/2005, 4 Ob 78/05g, http://www.internet4jurists.at/entscheidungen/ogh4_78_05g.htm (flirty.at); AU13. – OGH, 12/9/2001, 4 Ob 176/01p, http://www.internet4jurists.at/entscheidungen/ogh4_176_01p.htm (Fpo.at II).

[386] GE18. – OLG Hamburg, 20/2/2007, 7 U 126/06, http://www.suchmaschinen-und-recht.de/urteile/Oberlandesgericht-Hamburg-20070220.html; KG, 10.2.2006 – 9 U 105/05, NJW-RR 2006, 1481; GE21.– LG Berlin, 22/2/2005, 27 O 45/05, MMR 2005, 324; GE19.– LG Berlin, 9/9/2004, 27 O 585/04,

Most of the German decisions concern the liability of search engine operators for "adwords" chosen by customers of search engines in order to place their sponsored links so as to show up in user searches.[387] In a case dealing with trademark infringements[388] the court held that accessory liability[389] could only be considered where there was a gross and obvious infringement of a right or the search engine operator had been notified about the infringement. The court compared this principle to § 11 TDG[390], which exempts host providers from liability for damages provided that they remove third-party information or block access promptly after obtaining knowledge. Since the operator of the search engine had removed the advertisement using the title word "preispiraten" the court in the case saw no basis for applying the principles of accessory liability to the search engine operator. In a parallel case[391] an injunction could not be granted on the grounds of accessory liability[392], since the search engine operator had not violated any obligation to examine. A violation of the applicant's rights had neither been obvious (the case did not concern a famous trademark), nor could the defendant detect such infringements with reasonable effort. Given the very large number of keyword entries to be monitored and the continual convertibility of the words used as adwords, the search engine operator could not reasonably be expected to examine violations of trademark and competition law in advance. An injunction has been however granted in a online gambling case[393] where the defendant had operated a search engine which – unlike regular internet search engines – exclusively indicated websites of operators that were in a contractual relationship to the search engine operator. According to the court the operator of the search engine was obliged therefore to reject contract offers by online gambling providers that did not have a concession for Germany. In another case dealing with illegal online gambling[394] the search engine operator was found liable for unfair competition committed by the online gambling operator according to the principles of accessory liability, which presupposes the violation of an obligation to examine. An obligation to examine was deemed to be reasonable on the grounds that the search engine operator had had knowledge of the unfair competition over a longer period.

MMR 2005, 786; GE3. – LG Hamburg, 28.4.2006, 324 O 993/05, available at http://www.suchmaschinen-und-recht.de/urteile/Landgericht-Hamburg-20060428.html.

[387] OLG Hamburg , 4.5.2006 - 3 U 180/04, MMR 2006, 754, see also the trial court decision: GE22. – LG Hamburg, 21.9.2004, 312 O 324/04 MMR 2005, 631 ("adword"); GE23. – LG München I, 2.12.2003, 33 O 21461/03, MMR 2004, 261 ("adword"); GE24. – LG Hamburg, 16.9.2004, 315 O 755/03, MMR 2005, 480 ("sponsored link"); GE25. – LG Regensburg, 15.2.2005, 2 S 340/04, MMR 2005, 478 ("sponsored link").

[388] GE22. - LG Hamburg, 21/9/2004, 312 O 324/04, MMR 2005, 631.

[389] See Country Report Germany Part. 1 A I. 2..

[390] Implementing Art. 14 ECD; now § 10 TMG.

[391] GE 23. - LG München I, 2/12/2003, 33 O 21461/03, MMR 2004, 261.

[392] See Country Report Germany Part. 1 A I. 2..

[393] GE24. - LG Hamburg, 16/9/2004, 315 O 755/03, MMR 2005, 480.

[394] GE25. - LG Regensburg, 15/2/2005, 2 S 340/04, MMR 2005, 478.

3. Providers of Hyperlinks (other than Search Engine Operators)

a) National Regulations Concerning Providers of Hyperlinks

As for search engines, some member states (such as Austria, Spain and Portugal) have introduced, on their own initiative, specific regulations concerning information location tools, including hyperlinks.[395] Other member states apply their general principles of civil and criminal law to hyperlink setters.

b) Member States with specific regulations

The **Austrian** legislator introduced a special liability exemption for hyperlinks, which largely corresponds to § 16 ECG (referring to host providers). With regard to the provider's "embracing" of third party content (§ 17 (2) ECG: "the service provider presents the third-party information as its own") the explanatory memorandum of parliament refers[396] to the decision of the Supreme Court of Justice of 19.12.2000[397]. However, in contrast to the reasoning of the court, the legislator (parliament) explicitly stated that the *mere* setting of a link does not constitute an "embracing" of third party content. Hence, parliament refused to follow the logic and reasons given by the Supreme Court.

However, where the provider - depending on the individual circumstances - adopts the linked information or the linked information as his own, it does more than simply provide access to third party content and therefore may not enjoy exemption from liability.[398] There are no reported court cases dealing with hyperlinks since the adoption of § 17 (2) ECG.

Just as for search engines, **Spain** opted in its Law n° 34/2002 of July 11th, 2002, for a liability exemption for hyperlinks that adopts the same liability rules as for host providers - effective knowledge occurs only where notification has been given by a competent body. Injunctions are left untouched. In one case a court imposed a preliminary injunction[399] on the operator (and domain-holder/titular) of a website containing hyperlinks referring to p2p files. He had to remove the site from the network and had to insert this following text: "*This webpage has been blocked by a preliminary injunction in the context of a criminal lawsuit*". The decision made no reference to Article 17 of the e-commerce law establishing hyperlink providers' liability exemption. In another case[400] the condition of "actual knowledge" was not satisfied, even where the intermediary knew that a range of hyperlinks referred to illegal contents, on the grounds that it had not received any official notice from the authorities.

---

[395] Curiously, in contrast to the specific regulation for search engines in the ECSA Hungarian Law does not provide for any official definition of "hyperlinks", and consequently not for any liability exemptions.
[396] 817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP, zu § 17, http://www.parlinkom.gv.at/pls/portal/docs/page/PG/DE/XXI/I/I_00817/daten_000000.doc.
[397] AU10. – OGH, 19/12/2000, 4 Ob 225/00t, 4 Ob 274/00y..
[398] 817 der Beilagen zu den Stenographischen Protokollen des Nationalrates XXI. GP, zu § 17.
[399] SP10. – Decision (*Auto*) of the Examining Magistrate of Madrid, August 1st 2003, n° 5741/2002 – « EDonkey ».
[400] SP9. – Decision (*Auto*) of the Examining Magistrate of Barcelona, March 7th, 2003, DP 872/02-C – « www.ajoderse.com ».

Portugal's ECD implementing law provides for specific liability rules for intermediary service providers associated with content by means of search engines, hyperlinks or similar procedures (like directories). As a general rule, the intermediary is subject to the same liability as host providers (Provision 17). However, no court or administrative case has yet directly addressed hyperlinks. Nevertheless, one Portuguese administrative resolution ordered that all network content aggregation providers permitting a direct or indirect access to the incriminated website had also[401] to make impossible access. This ruling seems to cover, at least indirectly, hyperlink providers.

c) Member States applying general principles

In **Belgium**, courts have not (yet) excluded, in general terms, the application of the liability exemptions. The Belgian Supreme Court[402] held that the website owner (i.e. the domain-holder and operator of the website) containing hyperlinks referring to child pornographic contents had control and knowledge of these illegal hyperlinks even if the website owner did not insert them (hyperlinks were joined and proposed on the website). Consequently, the court refused to accord the host provider's liability privilege to the website owner. The judge stressed the purely technical and automatic character of the exempted activities, which implies that intermediaries cannot have knowledge of illegal content and have no control over it. On the specific facts before it, the court reasoned that the website owner had control and the knowledge of the contents to which the hyperlinks were directed (child pornographic content) – even though the operator himself had not placed the hyperlinks on the website. *A contrario*, we could deduct from the judge's interpretation that if the website owner did not have knowledge and the control of the illegal content, he would have benefitted from the host provider liability exemption.

In Germany the **German** Telemedia Act (TMG) does not apply to hyperlinks (the same position applies to search engines). The legislator recently rejected a motion by lobbying parties to extend liability exemptions to search engines and hyperlinks.[403] The German Federal Court of Justice has refused to apply the liability exemptions of the TDG and MDStV (today TMG) to hyperlinks[404]. Almost all lower courts have followed this ruling. Hence, there is no official definition of "hyperlinks" in German law. Even court decisions related to hyperlinks avoid defining the term, but there is a common understanding of a hyperlink as being a reference to another website. Accordingly courts apply the general provisions of civil, criminal and administrative law.[405] In a prominent criminal case, the Court of Appeal of

[401] PR1. – Administrative resolution from the National Authority of Communications (ANACOM) – 18.05.04.
[402] BE20. – Cour de cassation, 3 févr. 2004, *R.D.T.I.*, 2004, n° 19 ; En première et seconde instance : Tribunal correctionnel d'Hasselt, 1er mars 2002, *inédit* ; Cour d'appel d'Anvers, 7 oct. 2003, *A.M.*, 2004, liv. 2, pp. 166 et s.
[403] See Regierungs-Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr Vereinheitlichungsgesetz – ElGVG), Bundestags-Drucksache 16/3078, p 11 available at http://dip.bundestag.de/btd/16/030/1603078.pdf
[404] GE27. – BGH, 1/4/2004, I ZR 317/01, MMR 2004, 529 - Schöner Wetten.
[405] GE27. – BGH, 1/4/2004, I ZR 317/01, MMR 2004, 529 - Schöner Wetten; GE31. – OLG München, 28/7/2005, 29 U 2887/05, MMR 2005, 768 – Slysoft.

Stuttgart held, that as a general rule, setting hyperlinks to unlawful contents on the internet will suffice as a ground for criminal responsibility; in particular, direct linking will usually constitute a granting of access (as defined by criminal law) as a perpetrator.[406] However, setters of links might defend on the grounds of freedom of speech and civic education.

Cases in German civil law mainly concern injunctions on the grounds of copyright law or unfair competition law (in particular related to online-gambling). The German Federal Court of Justice[407] ruled that placing a hyperlink in an online version of a newspaper to a gambling website could be justified on the grounds of freedom of the Press (as granted in Art. 5 (1) of the German Constitution (Grundgesetz – GG))[408] as the link amended an editorial article. Until receipt of notice of the illegal content to which the link directed the user, the publisher (placer of the hyperlink) is not obliged to examine the linked content. The extent of monitoring and examination obligations of a person who places or perpetuates a hyperlink is subject to the general context in which the hyperlink is used, the purpose of the hyperlink, the knowledge of the person who sets the hyperlink of the circumstances (that imply that the website or internet-presentation serves unlawful purposes), and finally the resources at the disposal of the person who places a hyperlink to reasonably become aware of the illegality of this activity. The court explicitly confirmed that hyperlinks are an indispensable tool for the sensible use of the immense amount of information on the internet. However, the position changes when the setter of the link has been notified of the illegality of the content (or activity) to which the hyperlink refers. If the setter of the hyperlinks does not modify the link or simply deletes it he is contributing to the third party infringement and therefore might be held liable as well. Moreover, the general rules on injunctions apply here so that the setter of the hyperlink has to prevent future infringements such as linking to illicit content of the same manner.

In a case relating to copyright law the German Federal Court of Justice made reference to the socially desired functions of hyperlinks.[409] The court held that the placer of the link could not be held liable as an accessory, in the context of downloads by third parties that were linked to the website by the defendants' hyperlinks, as the defendant only prepared access to publicly accessible press articles. However, in another high profile case, the Court of Appeal of Munich found the placer of a link directed to hacker tools (software to remove copy protection devices) liable on the grounds of § 95a German Copyright Act (based upon the InfoSoc-Directive) since the placer of the link helped to advertise and disseminate the illicit content. This conclusion was reached regardless of the fact that the link was embedded in an article of an online newspaper, as the publisher (placer of the link) had received prior notice of the illegality of the content.[410]

[406] GE26. – OLG Stuttgart, 24.4.2006, 1 Ss 449/05, MMR 2006, 387.
[407] GE27. – BGH, 1/4/2004, I ZR 317/01, MMR 2004, 529 - Schöner Wetten.
[408] Grundgesetz für die Bundesrepublik Deutschland of 23.5.1949, BGBl. I S. 1.
[409] GE30. – BGH, 17/7/2003, I ZR 259/00, MMR 2003, 719 – Paperboy.
[410] GE31. – OLG München, 28/7/2005, 29 U 2887/05, MMR 2005, 768 – Slysoft.

According to **Dutch** law simple hyperlinks are legal even if they make reference to illegal content.[411] However, courts have issued injunctions against setters of hyperlinks,[412] such as in the case *Deutsche Bahn vs Indymedia*. In that case the court ordered a provider who hosted hyperlinks (set by third parties) to remove them since they referred to a site which contained *inter alia* injurious contents. The court considered that the website had to be compared to an access provider. In spite of the fact that the hyperlinks did not refer directly to the injurious contents (there were no deep links), the provider was ordered to remove them because it was well-known that the content was injurious.

Like other member states, the **UK** does not provide for explicit regulations on hyperlinks and for the time being sees no reason to regulate these.[413] This might be due to the fact that there are scarcely any reported court cases in the UK concerning hyperlinks. In one decision of the High Court[414], the judge held the placer of a hyperlink liable for the disclosure of indirectly confidential material hosted on another website, but only for the period after the setter of the link had became aware that the information published was confidential.

In **Polish** law it is still an unsolved problem whether and under what circumstances a person placing a hyperlink may be held liable for the illicit content of the website that the link leads to.[415] The question whether a hyperlinker has to examine the content of the website he links to for illicit content was dealt with in a case decided by a Court (Sąd Apelacyjny) in Cracow on 20.7.2004.[416] The court found that the defendant had praised the websites he had linked to and therefore had knowledge of their content. In the court's opinion, he must have visited these websites previously and noted their content. The fact that the defendant had no influence on the content of the website was irrelevant to the court since the defendant had recommended the websites. Most of the Polish legal literature has criticised this ruling, since it could result in a monitoring obligation for hyperlinkers. In contrast to the Cracow court, who deemed the placer of the link to be a direct infringer, the majority of Polish legal scholars[417] consider that a hyperlinker can be liable only as a helper under Art. 422 Civil Code (which requires the deliberate action of the helper - *dolus directus* or *dolus eventualis*). Hence, a person who sets a hyperlink may be held responsible only, if he was aware of the unlawful content on the site

[411] NE8. – Rechtbank 's-Gravenhage, 09/06/1999, Church of Scientology vs XS4ALL and others, LJN number AA1039, case number 96/1048, available via www.rechtspraak.nl; NE9. – Appeals Court of The Hague, 04/09/2003, Church of Scientology vs XS4ALL and others, LJN number AI5638, case number 99/1040, available via www.rechtspraak.nl; NE10. – Supreme Court, 16/12/2005, Church of Scientology vs XS4ALL and others, LJN number AT2056, case number C04/020/HR, available via www.rechtspraak.nl .

[412] NE7. – Court of Amsterdam, 20/06/2002, DB vs Indymedia, LJNnumber AE4427, case number KG 02/1073 OdC, available via www.rechtspraak.nl.

[413] See http://www.dti.gov.uk/consultations/page13985.html.

[414] UK6. – Queen's Bench Division, Master Leslie 26.1.2001 - Case No. HQ-000-1802 [2001] WL 98221 (QBD) - (Sir Elton John & Ors v Countess Joulebine & Ors).

[415] For a definition of hyperlinks cf. Prof. Barta/Prof. Markiewicz, Odpowiedzialnosc za odeslania w Internecie, [w:] Handel elektroniczny. Problemy prawne., Zakamycze 2005, s. 480- 481, Konarski, Komentarz do ustawy o swiadczeniu uslug droga elektroniczna, Warszawa 2004, Art. 14, punkt 12- s. 143.

[416] I ACia 564/04.

[417] Janusz Barta, Ryszard Markiewicz, Odpowiedzialność za odesłania w Internecie, [w:] Handel elektroniczny. Problemy prawne., Zakamycze 2005, page 486- 489.

his hyperlink leads to. Polish Criminal law equivalently regulates the culpability of helpers (dolus directus, dolus eventualis) in Art. 18 § 3 of the Polish Criminal Code.[418]

There have been only two reported cases in **Sweden**[419] which provide little guidance or general precedent given the particular factual situations they addressed. The Supreme Court found that a person who had posted hyperlinks to unlawful copies of music to be downloaded on a webpage was only making unlawful copies of the music available to the general public, and not copying the music (or helping to make copies of them). As the illegal making available to the public had not, at that time, been criminalized by Swedish copyright law, the accused was acquitted by reference to a provision in the Swedish Copyright Act (which state that public performances of recorded musical works are exempted from the exclusive right to works covered by the Copyright Act). The holders of such rights are, however, entitled to compensation under the Copyright Act.

Moreover, the Market Court (the highest instance for cases regarding unfair competition law and "market law")[420] found that it was not contrary to the Marketing Practices Act for a market place (Metro Marknad) to link directly to the classified advertisements of another market place (Blocket). Metro Marknad also planned to link to its own market place from Google, when the word "blocket" was entered as a search item. However, the court gave no specific reasons for its decision.

d) Deep Links

Deep links constitute a specific issue which have been the subject of several court decisions in various member states. Technically, a deep link is a kind of hyperlink referring directly to a file which is not situated on the homepage (root-page, the portal of entrance) of another website. The file is content which can be opened directly from the mother website. People browsing the mother website can, without doing anything more than clicking, open the content. Hence, any advertising or other offers or services etc. of the content provider (on his root homepage/website) can be circumvented by placing such a deep link.

At first, the **Danish** High Court held that deep linking was copyright infringement.[421] However, in 2006, the Maritime and Commercial Court of Copenhagen[422] overruled the previous decisions and declared deep linking practices to be legal as they are only technical tools.

This line of legal thinking is carried on by the famous "*Paperboy*" decision by the German Federal Court of Justice[423], which stated there was no liability for placing deep links to content in a database, as these links neither constituted a direct infringement of copyright or a

[418] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz.U. Nr 88, poz. 553, za rok 1997).
[419] SW4. – Högsta Domstolen, 15/6/2000, NJA 2000 s 292 - „Olssons Links".
[420] MD 2006:13.
[421] DE4. – Western division of the Danish High Court, 30/04/2001, *KODA*, available on the CD; DE2. – Copenhagen Bailiff's Court, 05/07/2002, DNPA vs Newsbooster, available on the CD.
[422] DE3. – Maritime and Commercial Court of Copenhagen, 24/02/2006, Danish real estate chain home vs Ofir.dk, available on the CD.
[423] GE30. – BGH, 17/7/2003, I ZR 259/00, MMR 2003, 719 – Paperboy.

contribution to third party behaviour. Deep links were described as being socially desirable information location tools, in particular as the database operator is able to protect himself by diverting all links directing to the specific web-site to the root site, i.e. to the main portal, so that his interest in earning advertising income can be satisfied by technical means.[424]

Similarly, the jurisprudence in the **Netherlands** has evolved from declaring deep links as illegal to permitting them. At first, Dutch courts deemed deep links to be copyright infringements,[425] as they caused copies. The Supreme Court held that copyright owners could forbid deep linking.[426] The uncomfortable situation was continued in a case concerning a content aggregator whose deeplinks were declared to be not illegal with regard to a search engine referencing MP3 files in the view of the Court of Haarlem.[427] However, the High Court of Amsterdam overruled this judgment.[428] The Court also declared that a search engine is not an internet service provider and thus that their liability regime could not be applied. Again, in another case (a few months after the ruling of the High Court of Amsterdam) the Court of Appeal of Arnhem disagreed with the Court of Amsterdam,[429] arguing that deeplinks, seen as pure technical links, cannot be classified as either inherently legal or illegal.

In contrast to these continental court decisions is one of the earliest decided cases in the **UK** (*Shetland Times*) concerning the use of a link to incorporate third party content into the operator's own publications, bypassing the first pages of the third party (and thus avoiding their advertisements). The court held that these links constituted an infringement of copyright under Section 20 of the Copyright, Designs and Patents Act[430] - a remarkable contrast to the German "*Paperboy*" decision.

III. Blogs and Internet Discussion Fora

In **France**, blogs are not treated unanimously by the courts: three categories can be distinguished. The first category contains blogs where the content editor only checks content (submitted by users) a posteriori. After the online publication, if needed/requested, the content

[424] GE30. – BGH, 17/7/2003, I ZR 259/00, MMR 2003, 719 (724) – Paperboy.
[425] NE18. – Rechtbank 's-Gravenhage, 14/01/2000, KPN vs XSO, LJNnumber: AA4712, case number: KG 99/1429, available via www.rechtspraak.nl .
[426] NE18. – Rechtbank 's-Gravenhage, 12/09/2000, NVM vs De telegraaf, LJNnumber AA8588, case number KG 00/949, available via www.rechtspraak.nl; NE20. – Gerechtshof 's-Gravenhage, 21/12/2000, NVM vs De telegraaf, LJNnumber AB0450, case number 00/1053, available via www.rechtspraak.nl; NE21. – Hoge Raad, 22/03/2002, NVM vs De telegraaf, LJNnumber AB0450, case number 00/1053, available via www.rechtspraak.nl.
[427] NE26. – Rechtbank Rotterdam, 22/08/2000, Kranten.com, LJN number AA6826, case number 139609/KG ZA 00-846, disponible via www.rechtspraak.nl.
[428] NE22. – Court of Haarlem, 12/05/2004, Technodesign vs Stichting Brein, LJN number AO9318, case number 85489/HA ZA 02-992, available via www.rechtspraak.nl; NE23. – Gerechtshof Amsterdam, 15/06/2006, Technodesign vs Stichting Brein, LJN number AX7579, case number 1157/04, available via www.rechtspraak.nl.
[429] NE24. – Court of Arnhem, 16/03/2006, NVM vs ZAH, LJN number AV5236, case number 136002, available via www.rechtspraak.nl; NE25. – Court of Appeal Arnhem, 04/07/2006, NVM vs ZAH, LJN number AY0089, case number A6/416, available via www.rechtspraak.nl.
[430] Court of Session: Outer House 24.10.1996 -1997 F.S.R. Shetland Times, Ltd. v. Dr. Jonathan Wills and Zetnews, Ltd.

editor will take some contents off. The content editor does not change the contents and does not choose what to put online. The second category contains blogs where the content editor check the contents a priori and decides if he will put the contents online or not. The content editor does not change the contents but decides what to put online. The third category contains blogs where the content editor modifies a priori the contents before putting them online.

Firstly, the Courts have considered people in charge of blogs and forums liable for the contents they host, following the Press law[431].

Then French jurisprudence distinguishes between the categories and the level of intervention. The TGI of Toulouse[432] explained that blogs (of the second category) are not liable if they promptly remove the allegedly illicit contents (principle of Duty of care). The TGI of Lyon explained that blogs and forums (of the first category) must follow the same legal regime as the Host provider [433]. Recently, the TGI of Paris has considered that the Press law has to be applied to the blogs (of the third category)[434].

Inter alia, the TGI of Paris had to specify the notion of "manifestly illicit". The court stated[435] that defamations (atteinte à la vie privée) are not manifestly illicit. In contrast, the Court of Appeal Paris[436] confirmed as manifestly illicit contents of racism[437], anti-Semitic propaganda[438], negationnism, revisionism[439], denials of war crimes, paedophilia images[440] and pornographic contents[441].

---

[431] FR39. - TGI Lyon, 28/05/2002, Chambre des Urgences, *SA Pere-Noel.fr c/ Monsieur F. M., Mademoiselle E. C. et SARL Deviant Network*. http://www.foruminternet.org/specialistes/veille-juridique/jurisprudence/tribunal-de-grande-instance-de-lyon-chambre-des-urgences-28-mai-2002.html?decoupe_recherche=p%C3%A8re%20no%C3%ABl
http://www.foruminternet.org/telechargement/documents/tgi-lyn20020528.pdf

[432] FR40. - TGI Toulouse, 05/06/2002, *Association Domexpo c/ SARL NFrance Conseil et Monsieur A. S.*
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=337
http://www.foruminternet.org/telechargement/documents/tgi-tls20020605.pdf

[433] FR41. - TGI Lyon, 14 ème Chambre, 21/07/2005, *Groupe Mace c/ Monsieur Gilbert D.*
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1027, http://www.droit-technologie.org/jurisprudences/TGI_Lyon_Correctionnel_210705.pdf

[434] FR42. - TGI Paris, 17/03/2006, *Ministère public, Commune de Puteaux c/ Christophe G.*
http://www.juriscom.net/jpt/visu.php?ID=803 http://www.juriscom.net/documents/tgiparis20060317.pdf

[435] FR43 = TGI Paris, 19/10/2006, *Mme H.P. c/ Google France*
www.juriscom.net/documents/tgiparis20061019.pdf

[436] FR 44 = CA Paris, 08/11/2006, Comité de défense de la cause arménienne c/ M. Aydin S., SA France Télécom services de communication résidentiels, http://www.foruminternet.org/telechargement/documents/ca-par20061108.pdf

[437] TGI Paris, ord. ref., 12 juillet 2001 http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord_tgi_paris_120701.htm

[438] FR33. - TGI Paris, 22/05/2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France.*
http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm
http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm#texte, FR34. - TGI Paris, 20/11/2000, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France*. http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.htm
http://www.juriscom.net/txt/jurisfr/cti/tgiparis20001120.pdf
FR35. - TGI Paris, 11/02/2003, *UEJF et Licra c/ Yahoo! Inc. et Yahoo France.*
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=621
http://www.foruminternet.org/telechargement/documents/tgi-par20030211.pdf

[439] FR1. - TGI Paris, 20/04/2005, *SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres*. http://www.juriscom.net/jpt/visu.php?ID=684
http://www.juriscom.net/documents/resp20050627.pdf ; FR2. - TGI Paris, 13/06/2005, *SA Tiscali, Telecom*

The notice-and-take-down-procedure concerning manifestly illicit content has to be followed meticulously and strictly. If not, the person responsible for the blog must be absolved of liability as no actual knowledge can be assumed.[442]

The debate about liability for blogs in **Germany** is inconclusive - there are scarcely any court cases to be found. A court in Berlin classified weblogs as being host providers in terms of § 11 TDG (§ 10 TMG).[443] The court denied liability for unlawful interference since it was neither reasonable for the weblog operator to control all contributions in advance nor to be aware of the falseness of the allegations made.

With regard to discussion fora, however, courts have had a greater opportunity to outline liability rules. The German Federal Court of Justice decided that there is no subsidiarity principle regarding injunctions[444] – in contrast to the position taken in France.[445] Even if the plaintiff has not tried to sue the author of a defamatory statement and even if the identity of that author was known to the plaintiff, he is entitled to sue for an injunction (not a preliminary one) against the operator of an online discussion forum in order to prohibit future defamatory statements. Hence, the operator has to control his fora to prevent these statements. Accordingly, the Court of Appeal in Hamburg stated, in a groundbreaking decision, that (onlinepress) operators of an internet discussion forum have to control their fora in the future if they received notice of illicit contents or a previous article posted by the operator himself had provoked illicit statements.[446] Thus, the court tried to strike a balance between freedom of speech and protection of victims' personal rights. Other courts have followed this ruling more or less closely.[447]

Courts in other member states have still had no opportunity to comment on the liability of blog operators (as host providers). Only two cases in **Spain** are reported,[448] considering

---

Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1139
http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf ; FR3. – CA Paris, 24/11/2006, *SA Tiscali, Telecom Italia, AFA, France Telecom et autres c/ UEJF, J'accuse, SOS Racisme et autres*
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1139
http://www.foruminternet.org/telechargement/documents/ca-par20061124.pdf

[440] Recommandation Les enfants du Net II : Pédo-pornographie et pédophilie sur l'Internet, 25 janvier 2005, http://www.forumInternet.org/recommandations/lire.phtml?id=844,

[441] Country Report France FR23. – TGI Paris, 27/02/2006, *Alain Afflelou / Google, Free*.
http://www.legalis.net/breves-article.php3?id_article=1648

[442] FR44. – CA Paris, 08/11/2006, Comité de défense de la cause arménienne c/ M. Aydin S., SA France Télécom services de communication résidentiels,
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=1114
http://www.foruminternet.org/telechargement/documents/ca-par20061108.pdf; TGI Paris, 19/20/2006, available on the CD.

[443] GE34. – AG Berlin-Mitte, 20/10/2004, 15 C 1011/04, MMR 2005, 639.

[444] GE5. – BGH, 27/3/2007, VI ZR 101/06, MMR 2007, 518.

[445] Note, however, that the principle of subsidiarity as laid down in Art. 6-I-8 LCEN concerns host and access providers, not directly the relationship between content provider (author etc.) and host provider.

[446] GE6. – OLG Hamburg, 22/8/2006, 7 U 50/06, MMR 2006, 744 - heise.de.

[447] See for example GE8. – OLG Düsseldorf, 7/6/2006, I-15 U 21/06, MMR 2006, 618; OLG Düsseldorf, 26.4.2006, I-15 U 180/5, MMR 2006, 553, overruled by BGH, 27.3.2007, VI ZR 101/06.

[448] SP12. – Decision of the Court of first Instance of Madrid (*Sentencia*), 00202/2006, 19.12.06, process n° 19/2006 – Case SGAE (General Society of Authors and Editors) against Frikipedia ; SP13. – Decision of the first Instance and Examining Magistrate of Arganda del Rey (n° 5) (*Sentencia*), 30.06.06, JF 134/06 –"Mafius

respectively the "wiki" operator and the blog author liable for defamatory or threatening messages. No judge to date has applied Article 16 of the e-commerce law (hosting activity) in favour of the operator of the blog website.

A somewhat different position was taken by the judge of the Tribunal of Madrid[449] concerning the owner of a website including many forums. An anonymous user opened a new forum and posted some defamatory messages against a well-known Spanish singer. The singer sued the website's owner. Following the judge's interpretation, provision 16 (host provider) has to be applied in this case concerning an information society service with third party content. Nevertheless, article 10 of LSSICE requires information society services to provide general information on their website (like the service provider's name, his geographical address, e-mail address, and so on, likewise art. 5 ECD). The concerned website only provided a general e-mail address, but not the name of the service provider, nor the physical address. The court considered that the requirement of providing this information is part of the diligence required by article 16 LSSICE. Since this information was not complete, the court deemed that the website owner was negligent and thus he could not benefit from the hosting exemption of art. 16 LSSICE. Therefore, he was held liable for the third party content.

IV. Content Aggregators and Web 2.0 (User Generated Content)

There are scarcely any reported cases on content aggregators and Web 2.0. This might be due to the fact that the notion of "content aggregators" is still not a legally recognised one, and that the interpretation of this notion seems to differ widely across member states. For example, some member states, such as **Germany**, concentrate on internet fora as virtual discussion rooms (again distinguishing between bulletin board systems (black boards) and real-time chat systems). Even in the one country (the UK) where content aggregators have been the subject of government consultation about the need to reform liability rules, no case law had been reported. Hence, it is not surprising that the DTI has found no reason to regulate them separately.[450] Other member states, like the Netherlands, deal only marginally with content aggregators.[451] According to one ruling[452], content aggregators are seen as host providers and are subject to their liability regime.

Only **Portuguese** e-commerce law provides for a specific liability exemption for intermediary service providers associated with content. However, Portugal obviously classifies search

Blog"; SP13bis. – Decision of the Provincial Court of Madrid (*Sentencia*), February 26th, 2007, 96/2007, (Appeal decision of the case Mafius blog).

[449] SP13ter: Decision of the Court of first Instance of Madrid, September 13th 2007, decision n° 184/2007.

[450] See http://www.dti.gov.uk/consultations/page13985.html.

[451] NE26. – Rechtbank Rotterdam, 22/08/2000, Kranten.com, LJN number AA6826, case number 139609/KG ZA 00-846, disponible via www.rechtspraak.nl; NE15. – District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031/HA ZA 05-211, available via www.rechtspraak.nl; NE16. – District Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, available via www.rechtspraak.nl .

[452] NE15. – District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031/HA ZA 05-211, available via www.rechtspraak.nl .

engines, hyperlinks or similar procedures as "intermediary service providers associated with content" (Provision 17 of the e-commerce Portuguese law) – which are treated as information location tools. Thus, under Portuguese law, the intermediary is subject to the same liability system as host providers. Provision 19 elucidates the scope of the liability exemption for intermediary service providers associated with content[453]. The law does not however define the notion of "intermediary service providers associated with content".

Most member states treat content aggregators (as classified here according to user generated content) as host providers, such as in the **Dutch** case of *Krantem.com*,[454] but without classifying or defining it, like in the case *Stokke BV vs Marktplaats BV*[455]. On the other hand, Dutch courts seem to make distinctions according to the extent of modifications made by the provider of the content provided by third parties, as in the case of *www.galeries.nl*[456]: Here the content aggregator was more than a host provider.

In a **French** case involving the web 2.0-platform DailyMotion (video sharing similar to Youtube) the TGI of Paris[457] recently declared DailyMotion to be a host provider and not an editor (in the press law sense). Nevertheless, the judge declared that Dailymotion knew about the contents. The website sells advertising and there is a link between popular contents and advertising incomes. DailyMotion put in place the circumstances for hosting illicit (but popular) contents. Therefore, there is actual knowledge of manifestly illicit contents. And because the contents were not promptly removed, DailyMotion was declared liable. The Court added that, even if a Host provider has no obligation to monitor, this exemption falls when the Host provider created the circumstances favourable for illicit activities. Therefore DailyMotion had to monitor the contents and remove the illicit videos by itself.

On the other hand, in a case concerning MySpace the TGI Paris recently stated that MySpace has to be regarded as a host provider, and also as an editor under press law,[458] similar to a

---

[453] "*1 – The association of content shall not be considered irregular solely through there being illegal content on the destination site, even if the provider has knowledge of this fact.*
2 – Remission is legal if it is carried out with objectivity and impartiality, representing the exercise of the right to information; and is illegal if it is represents a way of taking ownership of the illegal content for which remission was made.
3 – The assessment shall be carried out according to the circumstances of the case, in particular:
a) Possible confusion between the content of the site of origin and that of destination;
b) Automatic or intentional character of the remission;
c) Area of the destination site where the remission was carried out".

[454] NE26. – Rechtbank Rotterdam, 22/08/2000, Kranten.com, LJN number AA6826, case number 139609/KG ZA 00-846, disponible via www.rechtspraak.nl .

[455] NE26. – Rechtbank Rotterdam, 22/08/2000, Kranten.com, LJN number AA6826, case number 139609/KG ZA 00-846, disponible via www.rechtspraak.nl .NE15. – District Court of Zwolle-Lelystad (interim judgment), 03/05/2006, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031/HA ZA 05-211, available via www.rechtspraak.nl; NE16. – District Court of Zwolle-Lelystad (final judgment in first instance), 14/03/2007, Stokke BV vs Marktplaats BV, LJN number AW6288, case number 106031 / HA ZA 05-211, available via www.rechtspraak.nl .

[456] NE14. – District Court of 's-Hertogenbosch, 11/01/2006, Galeries.nl, LJNnumber AU9504, case number 126357 HA ZA, available via www.rechtspraak.nl.

[457] FR 48 = TGI Paris, 16/07/2007, Christian C., Nord-Ouest Production c/ DailyMotion SA SA UGC Images, http://www.juriscom.net/documents/tgiparis20070713.pdf

[458] FR 46 = TGI Paris Lafesse / MySpace, TGI Paris, Référé 22/06/2007, *Jean Yves L. dit Lafesse / Myspace* http://www.legalis.net/breves-article.php3?id_article=1965

previous case[459] regarding "Second Life". The court declared that the liability provisions of press law have to prevail over the liability exemptions of the LCEN by stressing the fact that MySpace generated revenues by hosting third-party content. In a LVMH/Vivastreet case[460], the judge qualified the website as a Host Provider. He gave an injunction of temporary monitoring obligations according to articles 6.I-7 and 6.I-8 LCEN.

V. Domain Name Services

In some member states a specific problem relates to the liability of information services: the liability of domain name operators who assign domain names to clients. Similar to the problems arising out of the adword system (or commercial links) used by search engines, the issue of trademark infringements and violations of rights to a name are crucial for these services. Moreover, not only top-level domain registrars are affected by this issue but also the so-called sub-level domain-providers, particularly if they are sued by third parties for infringements committed by clients to whom they offer access to the internet via their sub-level domain-system. In other words, these sub-level domain-providers are sued as access providers for infringements committed by their clients who engage in illicit activities under the second-level domain assigned to them through the services offered by the domain provider.

In **Austria** the "nic.at Internet Verwaltungs- und Betriebsgesellschaft mbH"[461] is the central registry for all domains under the Top Level Domain ".at". Decisions related to nic.at do not raise the question of the applicability of the ECG to domain name registries. Instead, as regards injunctions, the Supreme Court held that the registry nic.at is not subject to a general obligation to examine prior to or during the registration of a Second-Level Domain, due to the large number of registrations and the required automatic registration procedure. However, the registry is obliged to act in cases where the holder of a right can show facts and demands intervention, and where the infringement would be obvious to a non-lawyer without further investigation.[462]

In **Germany**, domain names are assigned by the German Network Information Centre DENIC[463] as the central registry for all domains under the Top Level Domain ".de". According to the German courts, the liability exemptions of §§ 9 to 11 TDG and §§ 7 to 9

[459] FR 47 = TGI Paris, 02/07/2007, Associations Union départementale des associations familiales de l'Ardèche et Fédération des Familles de France c/ Linden Research Inc, SAS Free, SA Neuf Cegetel et autres.
[460] FR48BIS. - TGIParis, 26/07/2007, LVMH c/ Vivastreet.
http://www.juriscom.net/actu/visu.php?ID=974
[461] http://www.nic.at/.
[462] AU13. – OGH, 12/9/2001, 4 Ob 176/01p, http://www.internet4jurists.at/entscheidungen/ogh4_176_01p.htm (Fpo.at II); AU14. – OGH, 19/12/2006, 4 Ob 229/06i,
http://www.internet4jurists.at/entscheidungen/ogh4_229_06i.htm (5thp.at).
[463] See http://www.denic.de/en/index.html.

MDStV (now §§ 8 to 10 TMG) are not applicable to DENIC since these provisions only refer to the provision of content.[464] Sub-domain-providers are being treated as access-providers in terms of § 8 TMG, since they grant internet access to third parties via their Second Level Domain.[465] Concerning accessory liability ("Störerhaftung") the German Federal Court of Justice restricts the obligations of Domain Name Providers, namely of DENIC, to liability for manifest infringements of trademarks etc. The Court emphasized the role and function of DENIC as a domain provider working in the interest of all internet users without pursuing its own purposes and commercial interests. Even after receiving a notice from an alleged right holder, DENIC is only subject to limited examination obligations.

Other countries define liability issues within the domain name system as a matter of contractual liability, as is the prevalent view in **Hungary**, where the Council of Hungarian Internet Providers (Internet Szolgáltatók Tanácsa - ISZT[466]) is the central registry for all domains under the top level domain ".hu". Exercising the possibilities for self-regulation provided in Act CVIII of 2001 (ECSA) section 15/A, the Scientific Association of Hungarian Internet Service Providers Council has established the Domain Registration Rules and Procedures [467](Regisztrációs szabályzat – RSZ) in order to ensure the uniform order of the delegation, registration and maintenance of public domains under .hu and to safeguard the rights of registrants and others. These Domain Registration Rules and Procedures have been issued as part of the contractual system in question. Only commercial registrars (providers authorised by the ISZT) are allowed to apply for a domain name. The liability exemptions of §§ 8 to 11 ECSA are not applicable to domain name providers. The Highest Court of the Republic of Hungary (Legfelsőbb Bíróság) has declared a registrar liable as a contributor to trademark infringements.[468].

In **France**, there has only been one ruling concerning a registrar. The TGI of Paris[469] held that a registrar is not a Host provider subject to Art. 6.I-2 LCEN. Therefore a registrar must not collect and keep identification data. At the same time, the court declared that the registrar had no obligation to check the personal details of his clients beforehand.

VI. Other Phenomena (Admin-C)

As far as can be seen, it is only in **Germany** that a specific liability issue has arisen. Some courts have discussed the liability of the "administrative contact" for infringements committed on websites operated by clients.[470] The "Admin-C" is a natural person appointed

[464] OLG Frankfurt, 14.9.1999, 11 U Kart 59/98, MMR 2000, 36; GE35. – BGH, 17/5/2001, I ZR 251/99, MMR 2001, 671 – ambiente.de, Also known as the "DENIC-decision".
[465] GE36. – LG Leipzig, 13/11/2003, 12 S 2595/03, MMR 2004, 263, the court wrongly uses „host-provider" as a synonym for „access-provider".
[466] www.iszt.hu.
[467] http://www.domain.hu/domain/English/szabalyzat.html.
[468] Fővárosi Bíróság 1. P. 29 766/2000/14 - BDT2004. 1068; Magyar Köztársaság Legfelsőbb Bírósága 2004 -Pf. IV. 25 696/2002/5 - BDT2004. 1068.
[469] FR49. – TGIParis, 25/10/2006, Participation Developpement Management c/ S.A.R.L. Gandi, disponible sur le cédérom.
[470] GE37. – LG Bonn, 23/2/2005, 5 S 197/04, CR 2005, 527; GE38. - LG Hamburg, 2/3/2004, 312 O 529/03, http://www.jurpc.de/rechtspr/20050024.pdf.

by the domain holder and authorised to decide all matters concerning a specific domain. Courts usually do not apply the liability exemptions of the TMG (E-Comm-Directive) to the Admin-C since they are not service providers in terms of the TDG (now TMG).[471] However, courts tend to deny any contributory liability for Admin-Cs (liability for unlawful interference) as they cannot control the content of the operator of the web-site.[472]

Part 2: Notice and Take-Down Procedures / Self- and Co-Regulation

The ECD explicitly encourages Self- and Co-Regulation, and the report stresses on self- or co-regulatory codes. However, it has to be noted that there is no pan-European accepted notion of "self-regulation" or "co-regulation". These terms are interpreted in different ways depending on the constitutional and legal tradition of each member state – and this has to be taken into account when assessing the degree of self- or co-regulation in each member state.

A. Codified NTD-Procedures

I. Finland

Finland is one of the few member states to have codified a complete and well-defined NTD procedure to prevent copyright infringements. The mandatory Finnish NTD is restricted to copyright and related rights infringements. The procedure is formal but easy to manage, and applicable to all three kinds of Intermediaries.

- Provisions regulate the service provider's contact point, form and content of notice.
- The procedure starts by notification to the service provider.
- The service provider must immediately prevent access and notify the content producer supplying him with the copy of the notification.
- If the content producer considers that prevention is groundless, he may get it returned by delivering to the notifying party a plea within 14 days. A copy must be delivered to the service provider.
- The content producer is liable to compensate damages caused if he gave false information in his counter notice.
- If the counter notice meets all the requirements, the service provider must not prevent the material from being returned unless otherwise provided by an agreement between the service provider and the content producer or by an order or decision by a court or by any other authority.

[471] GE39. – KG Berlin, 20/3/2006, 10 W 27/05, MMR 2006, 392; GE37. – LG Bonn, 23/2/2005, 5 S 197/04, CR 2005, 527; further: GE38. - LG Hamburg, 2/3/2004, 312 O 529/03, http://www.jurpc.de/rechtspr/20050024.pdf .
[472] KG op.cit.

When (section 16 of the Finnish Act corresponding to art. 14(3) ECD) a court orders a service provider to disable access to information stored by him, the content producer must also be informed.

The service provider and the content provider have the right to apply for reversal of the order (within the 14 days of the date when the applicant was notified of the order).

Ultimately, the procedure authorises a public prosecutor to appeal the decision that reversed the order.

During the preparation procedure for the implementation, the implementation of article 14 ECD has been controversial. According to the Finnish Constitutional Law Committee, the NTD might endanger the freedom of expression guaranteed by section 12 of Finland's Constitution[473]. Stakeholders would have preferred their own NTD[474].

Implemented in 2002, the NTD has been hardly used at all: "*As the NTD concerns only situations, where infringing material is hosted on ISPs´ server for their customer(s), the procedure is hardly used at all. NTD does not apply to p2p piracy, where the files are located on everybody's personal computer. We have no stats, if we had, it would be close to 0.*"[475]

II. Hungary

Hungary has implemented a "notice-and-take-down-procedure" in § 13 of ECSA dealing, however, only with infringements of intellectual property rights. This provision obviously follows very closely Sec. 512 of the US DMCA – however, the relationship to the liability provisions of the host providers (and Art. 14 ECD) remains unclear.

A holder of a right may request the removal of the information infringing his right by way of sending a notice in the form of a private document with full probative force or a notarised deed to the service provider. Following a notification the intermediary shall disable access to or remove the information identified in the notice within 12 hours of receiving the notice and shall concurrently give written notice to the affected recipient.

Within 8 days of receiving the intermediary's notice, the recipient of the affected service may lodge an objection with the intermediary, in the form of a private document with full probative force or a notarised deed. Upon receiving the objection the intermediary shall expeditiously make the relevant information accessible again and notify the right holder thereof, unless the removal of, or disabling access to the information was ordered by a court or authority. In the event that the affected recipient of the service admits to the infringement of the rights of the right holder or does not lodge an objection within 8 working days, or the

[473] The opinion of the Constitutionnal Law Committee of the Parliament, PeVL 60/2001 vp,p.3, available at www.eduskunta.fi .

[474] Finnish Copyright information and anti-piracy centre, Finnish Composers' Copyright Society, Business Software Alliance Finland and IFPI Finland to the Commerce Committee of the Parliament, on 19 February 2002, explained that a notification should not function only through a fixes-format notification but also through any other information that the service provider acquires of the existence of information infringing copyrights on his server.

[475] Comments from Mr Antti Kotilainen, Managing Director of the Finnish Copyright Information and Anti-Piracy Centre (CIAPC).

objection does not include the required content, the service provider shall maintain the effect of disabling access to, or removal of the information.

In the event that the right holder enforces his claim related to the infringement within 10 working days after being notified of the recipient's objection through a request for a court order or files a criminal report with the police, within 12 hours of receiving the court decision ordering interim measures to that effect, the service provider shall once again block access to, or remove the information. The service provider shall notify the affected recipient of the service of the measure that it has taken within one working day. The right holder shall advise the service provider of the final material decisions.

The service provider can not be held liable for the successful removal of, or disabling access to the relevant information, when the service provider has acted in accordance with the regulation of the procedure in good faith to ensure removal or disabling access thereto.

The Hungarian NTD procedure seems to be widely accepted and well functioning. Court decisions dealing with the interpretation of § 13 ECSA have not been reported.

III. Lithuania

On 22 August 2007, Lithuania has adopted the "Decree confirming the take down procedure as regards information acquired, created, modified or used in illegal manner"[476], which introduced a non-mandatory NTD with a right to counter-notice. The decree concerns all types of intermediaries and proposes two different categories of NTD with some formal differences. The NTD can be used by copyright owners in case of violation of their rights or. "if an individual notices information that he or she believes to be information which may not be published or distributed". Where the authorized institution has received a notice and has come to the conclusion that the information indicated is indeed illicit, the institution informs the service provider. The service provider has one day to decide if he keeps the content online or not. If the Service Provider ascertains that he or she is storing the information specified in the notification, and that the notification suitably meets the formal requirements, he must, within one working day of ascertaining the aforementioned facts, prepare a request to be sent, together with the received notification, to the Service Recipient at whose request he is storing the information alleged unlawful in the notification received, requesting that the Service Recipient assess the veracity of the information received in the notification. If the Service Recipient does not agree that the information received in the aforementioned notification is unlawful information, then within three working days of the date of despatch of the Service Provider's request, he must provide the Service Provider with a response.

If the Service Provider does not receive the Service Recipient's reply within the period of three working days, or if the Service Provider determines that the arguments presented in the

[476] Resolution N° 881 « Concerning Acceptance of a Report on Provisions for Eliminating the Possibility of Access to Unlawfully Obtained, Created, Amended or Utilised Information", http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_e?p_id=303361&p_query=&p_tr2= .

Service Recipient's reply are not valid, he must, within one working day of the expiry of the deadline for receiving the reply, eliminate the possibility of access to the unlawful information specified in the notification.

If the Service Provider doubts the veracity of the arguments presented by the Service Recipient in his or her reply, he may contact the relevant control body, requesting that it assess whether the arguments presented by the Service Recipient in his or her reply are valid. In this case the Service Provider must contact the relevant control body within one working day of evaluating the Service Recipient's reply. When the Service Provider receives a reply from the relevant control body, the deadline for evaluating a reply from a Service Recipient shall be counted anew.

If the Service Provider determines that he is not storing the information specified in a notification, or that the notification does not meet the formal requirements, he must, within one working day of receiving the notification, inform the individual who submitted the notification (if it is feasible to contact him or her from contact details held by the Service Provider) that he is not storing the information specified in the notification or about the deficiencies in the notification.

The Service Provider must store the unlawful information for which he or she has eliminated the possibility of access for not less than three months from the date of elimination of the possibility of access, except in cases where the Service Provider and the Service Recipient have agreed otherwise.

Following all these requirements, the Service Provider will not be liable. Nevertheless, this do not absolve the Service Provider from responsibility if he is himself in breach of the Republic of Lithuania Authors' Rights and Conterminous Rights Act, the Republic of Lithuania Design Act, the Republic of Lithuania Patents Act, the Republic of Lithuania Trademarks Act, the Republic of Lithuania Semiconductor Products Topography Rights Protection Act or the Republic of Lithuania Public Information Act.

IV. Spain

A preliminary draft of the bill « *Ley de Impulso de la sociedad de la Información* » originally planned an Article 17bis (Provision 17 referred to the liability exemption for the search engines and hyperlinks providers). The provision would have established a notification and take-down procedure in copyright matters. The provision was criticized and the Parliament abandoned the idea.[477]

V. Sweden

According to the Act on Responsibility for Electronic Bulletin Boards, the supplier of an electronic bulletin board is obliged to monitor the service regularly and in a fashion and to an extent that may reasonably be required taking into account the scope and nature of the service. In the event that the number of messages exceeds the host provider's capacity to supervise the

[477] Country report Spain SP 14.

bulletin board, the host is given an opportunity to comply with his obligation to supervise by way of a complaints page where users can report any irregularities.[478] This possibility however also presupposes that adequate measures are taken immediately as soon as the information is received. In practice however, the monitoring obligation is usually fulfilled by the provision of a complaints page of this kind.[479]

VI. The United Kingdom

With regard to criminal offences, UK law provides for a formal notice and take-down procedure in the Terrorism Act 2006[480]. Notices under section 3 of the Terrorism Act 2006 require the relevant person (as defined in section 3 (2)) to take down material on the internet and other electronic services that is unlawfully terrorism-related. According to the guidelines notices can be served on anyone involved in the provision or use of electronic services used in the publication or dissemination of terrorism-related material, including for example content provider, content aggregator, host provider, webmaster, forum moderator, bulletin board host, webmaster, etc..

The procedure in section 3 is connected with the offences in sections 1 and 2 of the Act in such a way that a person can lose the benefit of the defences in sections 1 (6) and 2 (9) where he does not comply with a section 3 notice. Section 3 (2) provides that persons served with notices who fail to remove, without reasonable excuse, the material that is unlawfully terrorism-related within the specified period (2 working days) are treated as endorsing it. Failure to comply is not itself an offence, but may lead to the provider being charged with an offence under the Act.[481] After Regulations 5 to 7 of the Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007[482] have come into force, hosts are only required to take down specified unlawfully terrorism-related material following receipt of a notice; they are not obliged to look out for and take down "repeat statements" pursuant to sections 3(4) to (6) of the Act. [483]

B. Self-Regulation

In more or less all member states there is some kind of self-regulation, i.e. a procedure which a provider uses in order to handle complaints about illicit content or access to illicit websites. In particular, eBay's so-called VeRO-Program is used in most of the member states – so that it will not be mentioned separately in each member state.

[478] We have received information on the following issues from the Swedish Ministry of Justice and the Swedish law firm Mannheimer Swartling.
[479] We have received information on this issue from the Swedish law firm Mannheimer Swartling.
[480] Available at http://www.opsi.gov.uk/acts/acts2006/ukpga_20060011_en.pdf.
[481] Guidance on notices issued under section 3 of the Terrorism Act 2006, No. 37.
[482] Electronic Commerce Directive (Terrorism Act 2006) Regulations 2007 (SI 2007/1550), available at: http://www.opsi.gov.uk/SI/si2007/20071550.htm.
[483] We have received a statement on this issue from the Department of Trade and Industry (DTI), cf. Part 1:B.I.3.

I. Austria

As one of only few countries, the Austrian Internet Service Providers Association (ISPA)[484] has developed a series of codes of conduct to substantiate the obligations following from the ECG. These codes of conduct are binding for the members of ISPA. The provisions of the code of conduct relevant to "notice-and-take-down-procedures" read as follows.[485] This code specifies the conditions under which a notice can be assumed, excluding anonymous request. However, the code does not provide any regulation regarding counter-notices.

II. Belgium

As in other member states, ebay Belgium has introduced the VeRO Program for protection of intellectual property rights.[486]

Belgacom has developed a voluntary collaboration procedure,[487] which involves a complaints notification to the public prosecutor (procureur du Roi). Belgacom reports the illegal content to the public prosecutor some days after having received the complaint. Every month, the operator sends also to the public prosecutor an electronic file containing automatic complaints. Where Belgacom hosts the illegal content, it blocks its access and asks his client to remove it. If the client doesn't remove by himself the illegal content, Belgacom does so.

Likewise, the Internet Service Providers Association (ISPA) has drawn up a code of conduct for cyber-criminality protection.[488]

The attempt of a Belgian judge in the Appeal Court of *Bruxelles*[489] should be mentioned. He has tried to work out a notification and take-down procedure in which the intermediary takes appropriate measures from the moment of the notification reception. The plaintiff ensures the intermediary's immunity if there is any complaint regarding his liability:

"[...] The respondents or any one of them must first inform BELGACOM SKYNET of these links by e-mail to the address indicated by it, must identify them stating the page(s) on the BELGACOM SKYNET customer's site on which these links appear and the musical recordings forming part of the repertoire of IFPI members that can be downloaded from the linked sites, and must expressly require that these links should be removed or made inaccessible[...]. Such notification should similarly expressly include the facts that would, prima facie, lead a reasonable ISP to assume that the files to which the links refer are illegal; BELGACOM SKYNET must remove these links or make them inaccessible within three working days following receipt of notification meeting the above conditions, unless it can show proof within the same period that the musical recordings to which the links complained

[484] http://www.ispa.at/.
[485] See http://www.ispa.at/downloads/1937e3c02fb2_Allgemeine_Regeln_zur_Haftung_und_Auskunftspflicht_des_ISP.pdf.
[486] BE24.
[487] BE25.
[488] BE26.
[489] BE17. – Tribunal de première instance de Bruxelles, 13.2.2007, www.droit.be, (CopiePresse c. Google); En première instance : Civ. Bruxelles (cess.), 2 nov. 1999, *A.M.,* 1999, pp. 474 et s. - SA Belgacom Skynet c. IFPI.

of refer are legal [...]. When submitting the request that links be removed or rendered inaccessible, the respondents must expressly accept that they will bear the responsibility for removing the links indicated by them or making them inaccessible and will indemnify BELGACOM SKYNET against claims that may be made by a customer on whose website hosted by it a link or links appear that are removed or made inaccessible on the respondents' initiative, should it subsequently appear that this was done unlawfully [...].”

III. Denmark

The Danish Telecom Industries Association has issued several codes of conduct on wrongful acts by users of the Internet and on the sheltering of immaterial rights[490].

IV. Estonia[491]

Very few access providers have set up an NTD procedure for copyright infringements that is accessible to the public. A greater number have separate agreements with copyright owners' associations.

V. France

Many self-regulatory codes of conduct have been issued in France. Leading associations have defined their codes of conduct. The most important are: CCI (chambre de commerce internationale), FEVAD (Fédération des entreprises de vente à distance), AFA (association des fournisseurs d'accès et de services Internet), BVP (bureau vérification de la publicité and ACSEL (Association pour le commerce et les services en ligne).[492] Most of these codes contain obligations of the members to install a complaint site or other instruments to report illicit contents.

VI. Germany

Self-regulation refers to codes of conduct that private companies agree to comply with. There are no codes of self-regulation concerning liability exemptions – with the exception of codes for protection of minors, which however do not explicitly address issues of liability.[493] Neither does any stakeholder, in particular business associations of providers, refer to any self-regulatory code of conduct of this kind.

VII. Spain

Nothing in Spanish law leads to any notification and take-down procedure: existing texts are restricted to only considering basic codes of conduct.[494] However, the music industry and universities in Spain have tried to establish a notification and take-down procedure. It is not

[490] Codes are available in Danish via : www.teleindustrien.dk/t2w_692.asp .
[491] Information from the Estonian Ministry of Economic Affairs and Communications, Internal Market Department. No more details were provided.
[492] See for more details Country Report France Case FR 55 ss.
[493] Cf. http://www.fsm.de/de/Beschwerdestelle and for the code of context; http://www.fsm.de/inhalt.doc/Verhaltenskodex.pdf.; http//www.jugendschutz.net.
[494] SP15.

clear whether any specific system has been adopted as a result. The lack of notice and take-down procedure in Spain can possibly be explained by the restrictive interpretation in Spanish law of the "effective knowledge" notion. Intermediaries' liability is not as quickly called upon as in other member states.

VIII. The Netherlands

Few self-regulatory initiatives have been initiated. One should mention however the VERO program from Ebay, which is a NTD procedure for reporting copyright infringements.

IX. The United Kingdom

Various self-regulatory bodies including ICSTIS[495] (which regulates premium rate telecommunications services) and the Direct Marketing Association[496] require compliance with laws such as the E-Commerce Regulations in their codes of practice. As in Austria, ISPA has issued a Code of practice which, however, does not contain a formal recommendation for notice-and-take-down-procedures but rather a kind of ombudsman procedure concerning complaints about a member of ISPA.

The Internet Watch Foundation (IWF[497]) is supported by industry and works with intermediaries on the restriction of access to illegal child abuse images hosted anywhere in the world and to content hosted in the UK of criminally obscene nature or that incites to racial hatred. The IWF is operating a hotline to enable the public to report instances of potentially illegal content and a notice and take-down service to alert hosting service providers of criminal content found on their servers. Full members (defined as having the ability to take down online content) agree to abide by the Members' Code of Practice[498] which describes how they will respond to IWF notices on potentially illegal content and the procedures when a member fails to comply with a notice.

Upon receipt of notifications from the IWF all full members agree to act within a reasonable time to take down the relevant content. They are obliged to inform the IWF if there are reasonable grounds for not reacting to a notice within a reasonable time, or if they believe an error has been made in the notice. Disputes arising over the assessment of whether content is potentially illegal are finally decided by the law enforcement agencies and prosecuting authorities.

C. Co-Regulation

The notion of co-regulation is understood as a kind of cooperation between private companies or institutions and public authorities in developing a regulation.

[495] http://www.icstis.org.uk/pdfs_code/11th_edition.pdf.
[496] http://www.the-dma.org/.
[497] www.iwf.org.uk.
[498] http://www.iwf.org.uk/funding/page.60.htm#newsgroup.

I. Belgium

The Internet Service Providers Association (ISPA) and the Ministries of Justice and Telecommunications signed a protocol of collaboration in 1999.[499] Consequently intermediaries have to notify illicit contents to the central point of contact, the "Federal Computer Crime Unit". The point of contact considers whether there is good reason for informing the public prosecutor of the issue.

IFPI sued Telenet (internet access provider) in 2004 for illicit contents infringing copyrights.[500] Finally, the parties settled during the procedure and concluded a protocol of collaboration. The protocol foresees a notice and take-down procedure, but the text is not accessible to third parties.

II. France

Many Co-regulation codes of conduct have been issued. The *Forum des droits de l'Internet*[501] and the French government are the principal bodies to have issued codes of conduct[502].

An important code of conduct for online auction platforms was issued on June 2006. Ebay, Amazon, PriceMinister, Alapage and 2xMoinsCher.com acceded.[503]

The AFNIC in charge of the .fr domain names has issued a "naming charter". In its chapter 12, it is clarified that a person or a company who wants to buy a .fr domain name must first check if the domain name does not cause any copyright infringement.

According to Art. 6.I-7 LCEN, French access providers and host providers (like Free, Wanadoo, OVH) established filtering mechanisms and procedures for notifying illicit contents.

III. Germany

There is no co-regulation[504] on the level of associations of German information society intermediaries or on the basis of agreements between individual Internet intermediaries providing for notice and take-down procedures in cases of infringements of intellectual property. However a kind of co-regulation standard exists for the protection of minors against illicit content. Internet providers participate in the Voluntary Self-Control Multimedia Services (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter e. V. – FSM[505]), an incorporated society founded by media-associations and Internet-companies. The members of

[499] BE21.
[500] BE22.
[501] FR60. – Publications du Forum des droits de l'Internet, http://www.forumInternet.org/recommandations/lire.phtml?id=1098.
[502] http://www.telecom.gouv.fr/rubriques-menu/organisation-du-secteur/coregulation/coregulation-Internet-412.html.
[503] FR67. – Charte de confiance des plateformes de vente entre internautes.
[504] Note, however, that from our perspective (according to the ECD) unilateral measures taken by just one provider (like eBay or Amazon etc.) are not encompassed by the notion of self-regulation. Hence, all programs like eBay's Verified Rights Owner (VeRO) Program, are not taken into account here.
[505] http://www.fsm.de/.

FSM have subjected themselves to a code of conduct[506] designed to prevent the dissemination of illegal content. The FSM is officially recognised by the Commission of the media-institutions of the Bundesländer for the protection of minors as regards telemedia-services (Kommission für Jugendmedienschutz der Landesmedienanstalten – KJM[507]). However, this code primarily targets issues of protection of minors rather than any general approach to monitor illegal activities on the web.

IV. Italy

The only relevant text is the Code of Connectivity Suppliers, formulated, under the aegis of the Federcomin trade associations (Federation of Information Technologies and Communication Enterprises)[508], AssTel and AIIP (Italian Association for Internet Providers). This Code has been signed by ISPs but not by copyright holders as it does not contain any provisions on notice and take-down. They have formulated amendments to the Code, but these amendments have not been accepted by ISPs. However, the Code has never been applied and it can be considered as a "dead letter".

[506] http://www.fsm.de/inhalt.doc/Verhaltenskodex.pdf.
[507] For the concept of regulated self-regulation see the official website of the KJM, http://www.kjm-online.de/public/kjm/.
[508] The name of Federcomin is now Confindustria Servizi Innovativi.