

eMarket Services makes it easier for you to use
electronic marketplaces for international business

eMARKETPLACES' LEGAL LIABILITY

By Teresa Rodríguez de las Heras Ballell
Associate Professor in Commercial Law
at the Carlos III University of Madrid (Spain)

www.emarketservices.com

May 2010

e-Business
Issue



Abstract

The rules of contractual and non-contractual liability are fully applicable to the activities carried out by the various operators on which the Internet's structure and operation are based. These are generally known as Internet Service Providers (ISP) and, in strict legal terminology, can be classified as Information Society Service Providers (ISSP).

In the absence of uniform EU (or international) legislation covering all aspects of liability in this context, we must resort to the applicable law resulting from the application of the rules of conflict of laws¹. All this is subject to the possibility that certain specific matters may be governed by treaties previously signed by Member States. This is the case of product liability which, in the context of e-Contracting, could be relevant in cases of direct trade or liability for defective software².

Liability: General Rules. False and Inaccurate Information

Therefore, taking into account that ISPs are subject to the general civil, criminal and administrative liability regimes which may apply pursuant to the rules of conflict of laws, cases of false or inaccurate information on websites must be resolved in accordance with the general rules of liability.

The problems arising from liability for false or inaccurate information are unrelated to their publication on digital media or electronic distribution. The difficulties which arise when applying non-contractual liability for damages caused by false or inaccurate information derive from the special nature of information as a public asset (non-exclusive use), the delicate establishment of causation based on people's trust in information, and the differences in the availability of compensation for purely financial loss (generally as a result of the false or inaccurate information).

In spite of everything, and even though providers are logically concerned about the issue of liability for the falseness or inaccuracy of their own contents, the true risks associated with carrying on their business online relate to activities, which might be referred to as intermediation activities, consisting of transmitting, providing access, hosting, caching, searching for, or linking to, third party contents. The risks arising from these activities can be difficult to predict, and their consequences can be particularly serious. Because of this, the

¹ In the context of European law, we must take into account the rules for contractual obligations laid down in the Rome I Regulation – Regulation 593/2008 of 17 June 2008 (OJ L 177/6, of 4 July 2008), which will be fully in force in late 2009, replacing the 1980 Rome Convention on the law applicable to contractual obligations – and, in the case of non-contractual obligations, the rules contained in Rome II Regulation – Regulation 864/2007 of 11 July 2007 (OJ L 199/40 of 31 July 2007), which has very recently come into force.

² See RODRÍGUEZ DE LAS HERAS BALLEL, Teresa, “La responsabilidad por *software* defectuoso en la contratación mercantil”, *Revista Aranzadi de Derecho y Nuevas Tecnologías*, issue no. 10, 2006, pages 83-110

laws of our neighbouring countries³ have designed a liability regime applicable specifically to intermediation service providers in order to deal with these situations.

Liability for Third Party Contents. Intermediation Service Providers

To analyse the liability of those providers who work with third party contents by transmitting, hosting, providing access to, caching, searching for, or linking to, such contents, we must first resolve a preliminary issue: identifying the intermediation service providers to whom the above mentioned specific regime would apply. Internet Service Providers provide their services in relation to the technological infrastructure, the information or the contents. Different types of operators can thus be identified based on their economic activities or in relation to the Internet. It is therefore a functional classification criterion which identifies providers on the basis of what they do rather than what they are or what they are like. This classification is fundamental for applying the rules of liability.

ISSPs can be divided into two main categories: general service providers or content providers and intermediation service providers.

Types of Information Society Service Providers

- Content Providers: These are online shops and newspapers, online travel agencies, e-banking providers, online ticket and flight booking sites, music download sites. In summary, these are the businesses which have chosen to open their windows to the online world, providing either their own contents or third party contents in relation to which they have some control and knowledge. For the purposes of legal analysis, the control-knowledge partnership is the distinguishing characteristic of this type of subject. To them, the Internet is not just a new goods and services distribution channel; it is a new arena in which to set up their business. The most accurate way of measuring e-commerce undoubtedly involves these operators' activities and performance. However, their actions depend on the efficient involvement of other subjects who support and manage the technical infrastructure and who organise and process the information, giving it added value and visibility, and conferring on it trustworthiness and credibility. These are the intermediaries.
- Technical Intermediaries: Technical intermediaries are characterised by the instrumental nature of their work: their services make it possible to operate the infrastructure underlying the Internet and are in one way or another linked to one of its structural elements: the information systems, the networks or the nodes. In relation to this, intermediaries carry out the following functions: access, carriage, hosting and caching. They are therefore the providers of access, the operators of networks and electronic communication services, the providers of hosting data services – generally known as servers – and the providers of caching services.

³ First, Section 512 of the United States Digital Millennium Copyright Act; soon to come, the European Union in Articles 12 to 15 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), (OJ L 178 of 7 July 2000, p.1), which has already been transposed into domestic laws.

From an information point of view, their functions are neutral or dispassionate. In other words, they only carry, provide access to, cache, or store, data which they neither generate, control nor are familiar with. They are simple intermediaries; they are the infrastructure which supports the Internet.

- Content Intermediaries: In spite of not being covered by any specific legislation, content intermediaries perform one of the most important functions in the online arena. They are the search facilities, the links, the portals, the indices, the forum managers and the e-marketplaces. They are intermediaries because their function is to sort, classify, give value to, localise, value, and assess, third party contents. Content intermediaries are the key to the operation of the Internet.

Risk Scenarios

As shown above, providers who provide their own content or who can at least know and control the contents made available by them assume no more risks than those taken by all subjects under the principle of liability for one's own actions (either direct actions or failure to properly instruct or supervise the party committing the harmful action). New risk scenarios thus arise when intermediation services are provided. This is because they involve transmitting, storing, copying, linking to, or searching, third party contents.

- a. Access and transmission
- b. Data hosting
- c. Caching
- d. Creation of links
- e. Use of search facilities
- f. Forum management and moderation (not envisaged in the legislation but socially relevant).

The risks assumed when carrying out activities which are key to the operation of the Internet have resulted in a number of scenarios called safe harbours under which, if the provider meets certain conditions, it will not be liable for user infringements. If it fails to meet any of these conditions, liability is not automatic or inevitable. Its possible liability must be analysed in accordance with the general rules of liability, which essentially require the existence of fault or negligence and turn around a harmful act resulting in a type of damage which gives rise to the right to compensation (act-cause-damage).

Rules of Liability for Third Party Contents

The rules of liability are therefore based on the following principles:

1. No liability: Intermediaries are not liable because they have no knowledge or control in relation to the third party contents they carry, host, cache or locate online.
2. However, as soon as they have actual knowledge of the unlawfulness of such contents, they must act diligently to either withdraw them or prevent access to them.

3. If they do not act diligently as indicated above, they will incur liability for their own actions; i.e. for any damage caused by their delay which increases the harm caused by the harmful action or prolongs its effects.

Specific Cases: Links

It's not that easy to equate the provision of links to other sites or to third party contents with other typical intermediation activities. This has resulted in several positions in the quest to clarify liability for contents on third party pages referred to by a link, based on whether the content sent is considered to be the content of the party providing the link or whether it is deemed to be third party content. Under the first position, the creation of a link is comparable with the activities carried out by access providers, where the lack of control over contents which characterises the latter's function means that there is no liability for third party contents in the case of links. This theory, however, is rejected by the majority due to the link creator's real possibility of knowing and assessing the content of the page to which the link refers. At the other end of the spectrum, however, is the position that states that, since establishing hyperlinks is a deliberate and voluntary action, the creator of the link assumes as its own the information to which it refers. However, grouping all the information linked to together with the link creator's information would put an excessive and impossible burden on the creator of the link to constantly supervise the content of the target page.

Rejecting these two positions on the basis that they are too extreme necessarily results in the creation of an intermediate position which analyses liability for third party contents on the basis of the type of link used (deep linking, inlining, framing). In deep linking, the link refers to a page inside the target site without going through the home page as an ordinary link would. In the case of inlining or framing, one or more resources or contents from another page are included in the page which generates the link. They are inserted in the website or its frame without any mention of the fact that the information comes from a third party. The above types of link entail the following risks as compared with ordinary links referring to a target home page: confusion regarding the origin of the information, the appearance of a business partnership between the two sites, potential infringement of industrial or intellectual property rights, abusive exploitation of third party contents and efforts, and even the assumption of liability as a result of the information linked to being false or inaccurate.

Risk Avoidance and Mitigation Strategies

1. **Informing users of the type of service provided and the terms of provision of that service:** For example, in the case of a search facility, users should be duly informed of whether it uses an automatic search engine or operates on the basis of search engine optimisation (SEO) contracts, and even the search and sorting criteria if appropriate. In addition, search results should be clearly distinguishable from sponsored advertisements.
2. **Implementing detection and withdrawal systems and systems for replacing withdrawn or blocked contents:** It is worth establishing exactly what information is required by the provider to act properly and duly inform its users of the criteria governing its operation, withdrawing information or blocking access and replacing withdrawn contents.
3. **Using ordinary links where possible:** If the use of deep linking, inlining or framing is advisable for cosmetic or commercial reasons, it is essential that the source of the contents be stated and, as far as possible, that users be given access, by means of a direct link, to the original website through its home page.

4. **Including, in a visible and easily accessible place, the content supervision and withdrawal policy:** This is particularly applicable in the case of moderated chats and forums. In the case of chats or forums with participant identification and access control, the rules governing participants' actions and the supervision and withdrawal policy must be included in the access agreement in order for contractual liability to apply.
5. **Including reasonable liability limitation or exemption clauses** or, in any event, clauses warning users of the limitations of the service (warning terms).