E-commerce - Ecuador

Principles of Liability of Internet Service Providers

Contributed by **Coronel & Pérez**

August 10 2006

Author

Juan Carlos Riofrío Martínez-Villalba

The liability of information service providers, such as internet service providers (ISPs), is a complex issue that must often be resolved under the law and jurisdiction of several countries. It is therefore necessary to analyze public and private international law.

The issue of ISP liability is frequently placed exclusively in the context of the publication of obscene or racist content. However, this narrow vision of informative liability (which subsumes the liability of information service providers) should be broadened.

Framing the Topic

Types of liability

There are several types of ISP liability. A classic division differentiates contractual liability from extra-contractual liability, which is based on the principles of law.

The following types of informative non-contractual liability depend on the type of right infringed:

- liability arising from the infringement of registered personal rights (eg, patents and trademarks);
- liability arising from the infringement of personal rights that do not need to be registered (eg, copyright and trade names);
- liability arising from the infringement of inalienable personal rights (eg, the right to one's name, honour, image and privacy); and
- liability arising from the violation of the rights of communities (eg, incitement to commit a crime or misdemeanour or incitement to armed revolt).

The following types of informative non-contractual liability depend on the type of regulation infringed:

- criminal liability;
- civil liability;
- liability arising under regulations for the protection of consumers or competition;
- liability arising under regulations for the protection of the rights of minors (eg, laws against child pornography); and
- other liabilities (eg, liability arising from the infringement of the right to family privacy or the inviolability of correspondence).

Legal framework

All countries possess a criminal, civil and administrative legal framework - some more extended and developed than others - which regulates this wide range of liabilities within the country's territory.

The provisions of national law that regulate informative liability usually concur in

condemning fundamental crimes and differ only with regard to punctual issues. For example, slander, deceitful conduct and child pornography are condemned worldwide, whereas Nazi and anti-semitic propaganda is not always prohibited.

The main difference lies in the way in which countries penalize or determine responsibilities for the infringement of regulations. Fines, prison sentences and the amount of compensation differ substantially from one country to another.

There are a great number of regulations on informative liability at national level. On the other hand, very few agreements deal with this issue on an international level - even though there are some honourable exceptions, such as the EU E-Commerce Directive (2000/31/EC).

With the advent of the information and communications technology era, pressure groups have sought to avoid the application of national regulations to the Internet. According to these groups, cyberspace should not be regulated by law. However, the Internet plays a significant part in today's world; it should thus be subject to rights and obligations in accordance with the law.

Substantive Principles of Informative Liability

Freedom of information

The governing principle of liability is freedom. Without freedom, there is no freedom of choice; without freedom of choice, no one can be held liable for his or her acts. On the other hand, freedom cannot exist without liability, as everyone must answer for his or her acts.

The fundamental right to information (which is recognized in several international agreements and constitutions) involves the ability to search for, diffuse and receive information.(1) The authorities must not interfere with the free circulation of information. Therefore, in most cases prior censorship is prohibited. Article 4 of the directive (principle excluding prior authorization) is a corollary of that principle.

Ex post liability

The right to information does not imply the irresponsibility or impunity of the media. *Ex post* liability arises after the diffusion of the information.

In some exceptional cases - which must be interpreted restrictively - it is possible to prohibit the diffusion of certain content (eg, copies made without the authorization of the copyright holder) or the creation of certain content (eg, the making of paedophile films). (2)

Principle of 'liable controller'

It is generally difficult to determine liabilities in the context of the provision of information. The key to resolve this issue is to admit that someone must be liable. The diffusion of information presupposes the principle of freedom of the informer - and, as a consequence, the informer's liability.

According to the general theory of liability, anyone who participated in a crime (authors, accomplices and accessories after the fact) may be held liable for it. The functioning of communication enterprises (including ISPs) usually relies on numerous employees (eg, photographers, reporters, salespeople and editors). All employees participate in some way in the publication or diffusion of the information; however, it would be unfair to hold them all responsible for an offence. Therefore, information law limits liability principally (and sometimes solely) to the person(s) directly involved in the infraction or damage.

Previously, the authors, accomplices and accessories after the fact could be held liable for a crime. For example, in the case of a slanderous political wall poster, the author, editor, publisher and owner of the advertising wall, among others, could be held liable. This regime of liability may have been justified by the fact that, in the past, a newspaper was produced, written and sold by only a few persons. This argument has now become out of date. The dimensions of communication enterprises (including ISPs) are such that it would be unfair - even impossible - to apply the former regime. For example, in the case of a slanderous television programme, it is more convenient to hold only one person liable (even though the cameraman filmed the offending scene, the editor failed to cut it, the media director failed to cancel the programme and the ISP failed to avoid diffusion on the Internet).

Various regimes of informative liability have existed in the past, including:

- liability by substitution;(3)
- the 'liable manager' regime;
- the 'liable editor' regime; and

- cascade liability (the most widespread system within the written press), which was created two centuries ago by Belgian law - only one person is presumed to be liable unless he or she can demonstrate that someone else was more directly involved in the offence.

With regard to ISP liability, the 'liable editor' regime first imposed itself. However, ISPs are now increasingly considered as mere distributors or libraries. Current technology does not allow ISPs to effectively control the volume of information introduced by its users. Moreover, the information cannot be controlled effectively without incurring disproportionate expenses.

The principle of 'liable controller' refers to the effective control of the information. If an ISP has the technical capacity to control the information effectively and uses this capacity, it can be held liable.(4)

Some ISPs save third parties' data automatically. They possess the technical capacity to control this data, but consider that it is not their function to do so. If ISPs have an 'effective knowledge' (in contrast to the mere automatic reception of the data) that certain information is illicit, they have a duty to inform the relevant authorities and withdraw the data (or make it inaccessible). If an ISP fails to report an offence, it becomes accessory after the fact; if it fails to withdraw the information, it becomes an accomplice to the infringement. The ISP's capacity to control information and its effective knowledge of the offence determine its obligations.

Principle of authenticity
ISPs and the information that they provide are subject to the principle of authenticity.(5)

Subjective authenticity implies that ISPs must identify themselves to their interlocutors. The principle of authenticity of the content is applicable to data messages. This principle is widely applied in several fields, including:

- commercial propaganda;
- non-requested commercial mail (which must identify the sender); and
- ideological information (the transmitter must admit its convictions).

The issue of authenticity is dealt with by national and international law, as well as in codes of ethics.

Principle of auto-regulation
The legislature aims to make information on the Internet (and in any medium) free, objective and truthful, but there is a limit to its powers. From that point, professionals must auto-regulate their activities. The legislature has thus established codes of ethics for professional associations. The law may oblige professionals to subscribe to these codes, but it cannot enforce its contents.

Adjective Principles of Informative Liability

Principle of state sovereignty
Many countries (mainly developing countries) have renounced their state sovereignty in this field because of the global dimension of the Internet and the significant technical, legal and economic hurdles faced in determining the liability of ISPs and enforcing penalties.

However, countries still have sovereignty to regulate, prohibit and penalize, among other things, false propaganda, deceitful advertising, trademark and copyright infringement and child pornography. Governments must enforce the principle of sovereignty over the information circulating within their territory, irrespective of its origin or source.

Principle of state liability
It is the *raison d'être* of the state (as established in several constitutions) to guarantee and protect fundamental human rights, including the right to information. The state is the custodian of these rights. State authorities or the state itself may be held liable for infringement of these fundamental rights.

Determination of the applicable law
Information may have its origin in country A and be received in country B, where an information provider multiplies its target. The message is then diffused in countries C, D and E, where it is posted on a webpage, which is accessible worldwide. Under which law should the liability of the information provider be assessed? In which jurisdiction should litigation take place?

In order to answer these questions, the following elements should be taken into consideration:

- Consumers have a right to assert claims in their own country and under the laws of their country. Claimants need only demonstrate the existence of a connection with this country for the national laws to be applicable. Therefore, liability for services provided in a certain country is limited by the legal system of that country. If services were provided in several countries, the laws of each of these countries would be applicable.

- Liability is usually governed by the law of the country where the unlawful act took place. With regards to civil crimes and unintentional tort, the obligations arising from crimes or misdemeanours are subject to the same law as that applicable to the crime or misdemeanours in question.(6) However, certain crimes are judged under the *lex fori.* Therefore, the law of the country where the regulation was violated applies to, among other things, the diffusion of content that is inappropriate for minors without any warning. It is nevertheless necessary to establish a sufficient connection with the country.

- Specific obligations required by law (eg, the obligation to make certain information available to the public) are governed by the law that set them forth.(7) Accessory obligations are governed by the law that regulates the main obligations.(8)

- With regard to criminal matters (eg, child pornography, diffusion of racist content and incitement to commit crimes, which is a criminal offence in certain countries), the general rule is the principle of territoriality.(9) No state shall apply the criminal laws of other states within its territory.(10) Where crimes have been committed in several countries, every country has jurisdiction to judge the crime under the Sánchez de Bustamante Code. In contrast, under the Montevideo Treaty, proceedings should be held only in the country where they were first initiated. However, where the crimes are related, the treaty grants jurisdiction to the country in which the most serious crime has been committed.

- IP rights that must be registered in order to be exercised (eg, patents and trademarks) are governed, in principle, by the law of the country where registration took place.(11) Nevertheless, numerous national and international regulations grant additional protection.

- The right to fair competition, which is based on the universal principle of good faith, is applicable worldwide in numerous sectors (eg, registered and unregistered trademarks), although certain countries do not have the capacity to enforce this right.

- Several treaties acknowledge the existence of fundamental rights. These rights may be invoked in national and international courts.

Comment

In the great majority of cases, the law of the process will be that of *lex fori*. Most importantly, the choice of the applicable law must comply with the rules of private international law.

Rather than creating new conflicts of competence, the Internet has multiplied the number of litigations; moreover, the burden of proof is now harder to meet. Therefore, there have been many calls for the creation of an international authority with competence to hear disputes arising from the diffusion of information on the Internet. A first step has already been made towards the resolution of disputes involving conflicting domain names.

Future policies must focus on:

- clarifying the rules of private international law;

- determining the law applicable to ISP liability; and

- ensuring that electronic evidence has procedural validity.

For further information on this topic please contact Juan Carlos Riofrío Martínez–Villalba at Coronel & Pérez by telephone (+593 2 2906 966) or by fax (+593 2 2523 306) or by email (jcriofrio@coronelyperez.com).

Endnotes

(1) Confer the Universal Declaration of Human Rights, Article 19; International Pact on Civil and Political Rights, Article 19; American Convention on Human Rights, Pact of San José de Costa Rica, Article 13. The doctrine and the various declarations of human

rights have established that the right to information involves the right to search for, receive and diffuse information (which can be exercised in a positive or negative way). Confer Ignacio Bel Mallen, Loreto Correidora y Alfonso and Pilar Cousido, "Right to Information", Colex, Navarra, 1992, page 111; and Escobar de la Serna, "Manual on Right to Information", Dykinson, Madrid, 1997, pages 53 to 63.

(2) There are numerous international regulations on child pornography and the degradation of children's dignity. See, for example: the Convention on the Use of Children in Pornography; the Convention on the Rights of the Child, Article 34; the Agreement on the Prohibition of the Worst Kinds of Child Labour, Article 3; the Agreement on the Protection of Victims in Armed Conflicts (Protocol I), Articles 75 to 77; the Agreement on the Protection of Victims in Armed Conflicts (Protocol II), Article 4; the Protocol Amending the Agreement on the Repression of the Circulation of Traffic of Obscene Publications.

(3) Under the regime of liability by substitution, the editor is liable where the author is unknown.

(4) The automatic treatment of information (eg, the filtration carried out by the administrator of a forum through a special software) shall not be considered as effective control. Such treatment of information is made by the ISP as a general rule; where the treatment of information is more specific, users shall be expressly informed in order to waive the liability of the ISP.

(5) According to the Cambridge Advanced Learner's Dictionary, "If something is authentic, it is real, true or what people say it is".

(6) See Sánchez de Bustamante Code, Article 167, and Treaty of Montevideo.

(7) See Sánchez de Bustamante Code and Treaty of Montevideo, Article 165.

(8) The doctrine widely accepts the solution proposed by the Treaty of Montevideo: the law that governs the main obligation also governs the accessory obligations.

(9) See Sánchez de Bustamante Code and Treaty of Montevideo. The treaties and the doctrine admits several exceptions to the principle of territoriality (eg, heads of states and their families, diplomatic personnel and members of the army). In those cases, the applicable law is that of the country of the person involved.

(10) See Sánchez de Bustamante Code, Article 296.

(11) See Sánchez de Bustamante Code, Article 115.