

Search

&gt;&gt;All Regions &lt;&lt;

North America

UK

Europe

Offshore

Asia Pacific

Latin America

 [Go]

Advanced Search

Login

Register for Free

First Time Here?

Mondaq Topics

Information Technology &amp; Telecommunications

RSS

&gt;&gt;Return to Homepage

Broadcasting Law  
E-commerce  
Information Security & Risk Management  
Information Technology Law  
Internet  
Licensing  
New Media  
Outsourcing  
Regulatory  
Software  
Telecommunications, Mobile & Cable Communications  
Year 2000

Anti-trust/ Competition Law

Banking and Financial

Construction, Property &amp; Real Estate

Consumer, Health and Family Law

Corporate/ Company Law

Environmental &amp; Energy

European Union &amp; International Law

Finance, Accounting and Consultancy

Government &amp; Public Sector Law

Immigration

Information Technology &amp; Telecommunications

Insurance and Transport

Intellectual Property

Labour &amp; Employment

Litigation, Arbitration and Dispute Resolution

Media &amp; Entertainment

Offshore

Pharmaceutical, Healthcare &amp; Life Sciences

Taxation

Press Releases

Our Services

About This Site

About

Testimonials

Common Questions

Contact Us

Feedback Form

Privacy Statement

[Northwest Indiana Lawyers](#)

Professional Highland, IN Law Firm. Get Just Compensation for Injuries.

[Constuction Expert](#)

Construction Expert testimony and demonstrative presentations.

Ads by Google

## Hofer Loesch Torricelli

### Italy: Web Content, Personal Data Handling, Free Speech, Providers' Liability In The Internet Environment

19 April 2007

#### Article by Felix Hofer

#### Article by Avv. Felix Hofer<sup>1</sup>

1. In recent years Internet Provider's liability has more and more shifted to the centre of an intense debate involving exponents of conflicting interests.: *Pressure Groups* are active lobbying for industry's or businesses' (economic) interests or advocating in favour of widely recognized principles (freedom of speech, no barriers to information, pluralism, cultural exchange, etc.). *Politicians, Regulators, Public Authorities and Watchdogs* usually tend to focus on providing some kind of viable legal framework for international relations as well as on trying to meet needs of common/general interest (safety, crime prevention, intelligence, preventive control, etc) or on granting adequate protection to sector groups/interests (consumers, children and minors, etc.). *Providers* struggle with: (a) delivering services characterized by sophisticated (and rapidly evolving) technology, (b) moving into areas where traditional "rules" and existing legal framework often result widely inadequate for dealing with the arising new issues/problems, and (c) facing interference and reactions from all the other players in the game (frequently lacking of a sufficient level of familiarity the technical aspects involved by the questions at stake). Last but not least the *Internet Users* feel both, being targeted from all the other players mentioned above as well as deeply attracted by the potential of the services offered by new technologies<sup>2</sup>, but also consider themselves as being "invaded" by new technology's practical application<sup>3</sup>.

Additional action is brought onto the scenario by legal experts and courts, called in to disentangle complex conflicts of interests.

2. Most of those players in the game have just one aspect in common: they face enormous difficulties in properly understanding the technical implications involved by the use of electronic means and therefore truly struggle when required to provide solutions for totally new problems and when trying to apply their proven – but traditional – expertise to new devices, mechanisms and services.

It's not that long ago when courts were involved in comprehensive discussions about the "legal" nature of a website and were wondering whether a site should be assimilated to a "newsstand" or rather to a "publishing house".

3. While huge efforts had to be performed for coming across disputes and litigation in cases where the parties were located everywhere, used to target everyone and where jurisdiction and enforcement frequently resulted in riddles with almost no solution, another problem rising aspect added itself to an already sufficiently complex and messy situation: with businesses shifting to the Internet, electronic communication became, firstly, more and more popular and then crucial, especially for marketing purposes.

But electronic communication necessarily implies collecting, storing, handling, transferring, profiling, in short, "processing" of personal data by a wide range of different subjects, as agencies, advertisers, media companies, Internet providers, call centres, research companies (and many others), which subsequently face new and specific liabilities.

4. In the beginning this appeared to be just an additional (even if somehow annoying), mainly formal obligation to fulfil, but very soon how to comply with both, national and international regulation (i.e. the specific EU Directives) on personal data processing turned out as a major practical and legal problem for companies in their domestic businesses as well as in their cross-border economic relations.

In fact, the Data Protection Commissioners in the EU member countries (i.e. national, independent Authorities, in charge of the Directive's domestic implementation) started focusing their attention on new techniques, means, devices and services, as: SMS, E-Mail or Electronic Ads (e.g. Pop up Ads), Cookies or "web bugs" (mini bits of code left on user's PCs), Banners, Java Scripts, Spy Ware (key logging), RFID (radio frequency identification) tags inserted in packaging, loyalty cards, smart shopping trolleys, clothes, monitoring (low-level radiation cameras to "see" through clothing, walls or cars).

Those Commissioners:

- coordinate on a trans-national level<sup>4</sup>,
- concentrate not only on subjects established in the EU, but
- extend their control on foreign subjects using, while processing personal data, equipment located in the EU's territory,
- claim for special codes of conduct (meant to rule data processing on the Internet, data recording through audiovisual systems, data use in Direct Marketing),
- do apply sanctions (usually fines, but violations of privacy rules can result also in criminal offences, punished with imprisonment up to 3 years).

5. A quick glimpse on some cases handled by Courts or Authorities throughout Europe and in other foreign jurisdictions delivers a neat idea about how tricky and nasty legal implications linked to handling of personal data can turn out. Sometimes the impact of data processing issues on businesses - or on entire business sectors – can result extremely worrying.

#### 5.1. Germany:

A first instance Court in Berlin<sup>5</sup> had to deal with a complaint about receipt of unsolicited commercial communication. The plaintiff had registered his cell phone number with an IS provider, offering to its clients a free SMS messaging service. The provider had passed on such data – without the cell phone holder's consent - to another company, which used it for running an advertising campaign performed via SMS.

In its decision<sup>6</sup> the Court found that a violation of the provisions on data protection had occurred, issued a cease injunction against the two providers involved and fixed an eventual fine of 250.000 Euro for non compliance with the desist order. It also awarded 7.500 Euro as damage compensation to the plaintiff for the three unsolicited e-mails received<sup>7</sup>.

#### Free Personalized News Alert

Would you like to be kept informed about similar articles? >Signup<

#### Related Information

##### Information Technology & Telecommunications

Information Technology Law  
Internet  
Telecommunications, Mobile & Cable Communications

#### Related Functions

- Ask the firm/author a question
- Email a colleague with a synopsis and link to this article
- Updated Printer-friendly version of this page
- Bookmark this Article.

Ads by Google

[Construction Expert](#)

Construction Expert testimony and demonstrative presentations.  
[www.SynergenConsulting](http://www.SynergenConsulting)

[Fast Breach Recovery](#)

Kroll: for quick, complete recovery  
 Prevention of future breaches  
[www.krfs.com](http://www.krfs.com)

**5.2. Italy:**

A Professor received a promotional message sent to an e-mail address, available on the University's web site. He filed a complaint with the local Data Commissioner arguing that his address was listed on the website "for institutional purposes" only and he therefore felt that improper (commercial) use of his personal data had been performed.

The advertiser objected that the listing of the address in a 'public' directory (i.e. on the University's website) allowed public use of the data.

The Italian Privacy Commissioner stated<sup>8</sup> that:

- the fact that personal data could be found on the Internet didn't make them publicly available,
- therefore the specific purpose pursued through data's diffusion on Internet resulted relevant,
- in the specific case, the e-mail addresses being available on the University's website only for a 'limited purpose' (the institutional one), their use for sending commercial communication was not allowed without achieving data subject's prior consent.

In another case a bank's client, regularly receiving - despite explicit denial of consent for being targeted with unsolicited commercial communication - advertising material attached to his statement of account, complained with the Privacy Commissioner about such practice.

The Bank argued to its defence that the questioned marketing material had been sent for informative-educational purposes<sup>9</sup> and that commercial communication other than that had to be considered as just 'marginal' and not likely to change the messages' main - informative - purpose.

The Authority in its decision<sup>10</sup>:

- found that the bank had acted illegally by sending - against the addressee's specific will - promotional material to an address extracted from its business database,
- felt that, illegal personal data processing potentially resulting in a criminal offence, the bank's illegal conduct required the case being transferred to a criminal prosecutor for evaluation of the bank's business practice.

**5.3. United Kingdom:**

A leading UK retailer decided to start testing - in a shop located in Cambridge - the effectiveness of tracking chips inserted in the packaging of a specific product (razor blades). At the moment the product was removed from the in-store shelf the chip switched a CCTV camera on, while a second picture was taken at the checkpoint.

Unfortunately this test procedure - even if clearly performed for security reasons - became public and steered angry reactions from shoppers who felt they were being targeted with an unacceptable privacy invasion. Protest actions were organized outside the retailer company's stores and the razor blade producer was asked to remove the chips from its packages. A representative of a civil rights group expressed concern about potential "functions creep"<sup>11</sup>.

Even before legal action was taken the retailer rushed to publicly declaring that the company had absolutely no "intention of using this technology to track, videotape or photograph consumers" and stressed the importance of RFID for solving perennial business problems such as shoplifting, inventory shortages and logistical errors.

On September 10th, 2003 the Advertising Standards Authority - ASA issued its first landmark decision with respect to the meaning of "specific consent", required - under the new privacy regulation - for using marketing lists and for targeting consumers via e-mail campaigns. The decision also delivered useful indications as to identifying 'marketing communication'.

The case originated from the marketing practice of a Southampton based seminar organizer, who started sending unsolicited messages under the headline: "Business Seminars - Telesales & Selling Skills Made Easy". When opened, the message resulted actually intended to promoting a "sales course for non-aggressive people".

A complaint was filed with the ASA for infringement of the CAP code, raising two issues: (a) that from the e-mail's subject line it was all but clear that a marketing communication was the content of the message, (b) no explicit consent from the addressee had been sought out - and received - before sending the message.

The ASA considered that the reference to "Business Seminars - Telesales & Selling Skills Made Easy" allowed to easily identify the message as a marketing communication, but also held that after March 2003 such communication could not be legitimately sent - not even to existing customers - without an explicit prior consent from the addressee.

The defendant's argument that a mailing list of subjects willing to receive promotional e-mails had been used was not considered as relevant.

**5.4. United States/Italy:**

A renown Italian clothing producer found itself in trouble when the company announced that it was interested in testing, in some of its US shops, RFID technology and stated - in a joint press release with the tag provider - that the particular device would result "imperceptible to the wearer and remain in individual items of clothing throughout their lifetime".

When press reports assumed that the company had embedded tracking chips in its clothing, advocates from a US consumer protection group<sup>12</sup> invited consumers to boycott, on a worldwide basis<sup>13</sup>, the company's products and warned that the chips could be used for more than just unwanted advertising, being able to link customers' data as name, credit card information to the serial number of the product and to track the "identified" subject any time he/she approached a tag reading device.

Rather surprised by such - apparently unexpected - opposition, the company performed a sort of U-turn and rushed to explaining that, "always having been a leader in technological innovation in the clothing sector", it was simply analysing RFID technology in order to evaluate its technical characteristics and emphasized that no feasibility studies had been undertaken with a view to the possible industrial introduction of this technology".

Interestingly, another famous Italian cloth producer, using RFID technology in its Manhattan shop since 2002, had succeeded in going away with such practice without any significant reaction from consumers.

**6.** By then the time had come for some harmonizing efforts aimed at achieving a common view on the new aspects of personal data handling in electronic communication.

To this purpose the Data Protection Working Party issued<sup>14</sup> some additional indications as to the impact of the EU data protection Directives on data processing performed web sites not located within Union's territory as well as to protection offered to individuals not being EU citizen.

According to this opinion, the provisions of EU Directive no. 95/46 imply that national law becomes applicable:

- when data processing is carried out by an establishment's activity<sup>15</sup> based within the territory of a Member State<sup>16</sup>,
- if a data controller, not established on Community's territory, makes use of technical equipment, automated or otherwise, situated within the territory of a Member State<sup>17</sup>.

In the DPWP's reading, 'disposal'<sup>18</sup> of technical equipment has to be intended in the sense that:

- not ANY interaction between an EU Internet user and a web site based outside the Union's territory implies application of the Directives,
- to this purpose relevant is the fact that the equipment is at controller's disposal for processing of personal data,
- -as to the extent of disposal, not full control on equipment is necessary, but a sufficient degree of disposal occurs, if the data controller, in determining the way that the equipment works, makes relevant decisions as to data handling's procedure<sup>19</sup>.

The DPWP's opinion steps on to dealing with specific technical details characterizing electronic communication by affirming that:

- 'cookies'<sup>20</sup> used for data collection on a PC's hard disk may result relevant for assessing the law applicable and require both, proper in-advance notice<sup>21</sup> to data subjects about the information stored, it's purposes and validity period as well as offer of an acceptance option,
- 'Java Scripts'<sup>22</sup>, allowing remote servers to run applications on a user's PC and apt to be used for: (a) collecting and processing personal data stored in user's PC, (b) providing customers with most „adequate" banners or ads, (c ) for "profiling" without user's awareness, results in a form of invisible and not legitimate data processing,
- 'Spy wares'<sup>23</sup>, sending back personal information related to the data subject<sup>24</sup> also do result in illicit processing of personal data.

**7.** The issues mentioned in the previous paragraphs necessarily brought the debate around electronic communication, web content and personal data protection to focusing on Provider's liability. The reason for such outcome is fairly obvious: when dealing with unfair practices performed on the Web, the key question faced by regulators, watchdogs, Internet businesses and their clients always is *"How to get the bad, guys, how to enforce legal provisions or judicial decisions against them?"*

Despite the fact that everybody in the game is strongly convinced that finding a viable answer to that problem is crucial to the future of on-line businesses, up till now nobody succeeded in coming up with a truly satisfying solution.

Therefore the temptation of choosing to proceed on the easiest track resulted really huge and Providers found themselves quickly exposed to the attention of those desperately looking for somebody to blame (and to sue). Actually Providers constitute an appealing target to that purpose as they can be located, reached and caught; in addition they usually offer sufficient financial strength and tangible assets, fundamental aspects for plaintiffs seeking damage compensation and trying to enforce court decisions.

Obviously Providers were not exactly happy to find themselves put *"between the hammer and the anvil"* and to take liability for malpractice frequently out of their control. Lobbyists specific representing pressure groups, advocates of the freedom of information principle and people objecting to excessive control over the Internet and content posted there started drawing Legislators' attention on the problems and difficulties to be faced when trying to establish a harmonized legal framework meant to "rule" the Internet. .

Well aware of those objections the EU's Committee of Ministers issued<sup>25</sup> the *"Declaration on freedom of communication on the Internet"*, recommending that:

- the Internet should not become subject to restrictions, which go further than those, applied to other means of content delivery,
- self-regulation or co-regulation should be widely encouraged for ruling content dissemination on the Internet,
- in principle<sup>26</sup>, public authorities should not deny<sup>27</sup> access to information and to other communication on the Internet, regardless of frontiers,
- existing barriers for accessing Internet communication and information services should be removed,
- freedom should be granted as to providing services via the Internet,
- no general obligation should be imposed on service providers as to monitoring of content, which they give access to or they transmit or store; neither should providers be held liable for content on the Internet when their function is limited to transmitting information or providing access to the Internet,
- while co-liability may hit them where they do not act expeditiously to remove or disable access to information or services as soon as they become aware of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information,
- for enhancing the free expression of information and ideas, the will of users of the Internet not to disclose their identity should be respected as long no responsibility for criminal acts is involved.

**8.** So far so good, but did Providers' uncomfortable "black sheep" position actually change after the formal declaration of those noble principles? Had life in Court become easier for Providers?

### **8.1. United States:**

A U.S. Court of Appeals<sup>28</sup> delivered an interesting decision on provider liability. The case dealt with by the court involved a company operating a dating site and originated from the fact that a fabricated profile of an L.A. based actress contained real data (as name and address) combined with falsehoods.

The company operating the site found itself involved in the lawsuit because of the interactive nature of the questionnaire generating the posting.

The Court of appeals held that<sup>29</sup> *"So long as a third party willingly provides the essential published content, the interactive computer service receives full immunity regardless of the specific editing or selection process"*<sup>30</sup>

### **8.2. Germany:**

Dealing with a controversy around domain name registration, a German second instance court<sup>31</sup> was faced with the following facts: two companies active in the foodstuff sector (sweets), one as the trademark owner, the other as the product's distributor, jointly sued a Provider (in charge of the assignment service of domain names and of the respective IP address numbers).

The plaintiffs alleged that undue registration - in favour of third party - of an Internet domain corresponding to its trademark<sup>32</sup> had been performed, as the questioned domain had been assigned to a company in Malaysia, while previously a WIPO arbitration panel had decided for re-assignment of the domain name in favour of the German company owning the trademark.

The plaintiffs (at this stage primarily seeking for recovery of legal costs) assumed that Provider, by assigning the domain to the Malaysian company, had infringed on the German Trademark Act<sup>33</sup>.

In his defence the Provider argued that the enormous number of applications filed made it objectively impossible to perform a case-by-case check as to potential violations. Therefore it didn't appear reasonable to expect a Provider to perform such specific and in-depth control.

In its decision<sup>34</sup> the German Court accepted the defendant's argument and held that no co-liability could be found originating from the defendant's service and therefore dismissed the claim.

**9.** Providers' business appeared to have become more comfortable when the EU Directive on E-commerce<sup>35</sup> was issued, setting some basic principles on liability.

Italy performed the Directive's implementation through detailed provisions<sup>36</sup>, which:

- set (as a general principle) that providers do not bear a general obligation of controlling the information transmitted or memorized on their servers<sup>37</sup>,
- establish an identical exemption<sup>38</sup> of content control and of liability with respect to "mere conduit" providers<sup>39</sup> as well as for automatic, intermediate or temporary memorizing (caching)<sup>40</sup> as long as the provider does not modify the information's content, complies with terms and conditions for accessing and updating the information, does not interfere with the client's use of technology for profiling or data collection purposes, promptly removes the information once it's no more present in its original location,
- finally confirms<sup>41</sup> such exemption also for permanent or long term information storage as hosting services performed by a third party<sup>42</sup>.

**10.** Everything clear and settled at this point? Not really! At least this is the neat impression one gets when looking at some local case-law and at some recent initiatives taken by Regulators.

**10.1.** Recently the public opinion in Italy was shaken by an episode of "bullying", which involved a group of minors who recorded themselves with a mobile phone while harassing and beating a young disabled. The video was then posted on a web portal (in the Section "Funny Videos"!).

*Vivi Down*, a local not-for-profit organization, assisting people affected by Down's syndrome, became aware of the existence of the video, felt that the episode resulted in a criminal offence and therefore brought the facts to the attention of the AG in Milan.

The AG decided to extend his inquiry about eventually performed criminal offences against two of the web portal's country managers. This despite the fact that the search engine, when informed about the questioned posting, had arranged for the video's immediate removal (even before the AG had taken action).

The national press reported widely about what happened and an intense debate heated up, involving the general public as well as legal experts and politicians (calling – once more – for stricter control on Internet content).

While the episode itself clearly left no space at all for disagreement (nobody obviously intending to question the need of immediate action against the youngsters responsible for the bullying), the discussion focused on the legal aspects implied by the proceeding against the search engine's country managers.

A spokesman of the Internet company stressed that, once achieved awareness about the episode, instant action had been taken in order to remove the video and unconditional cooperation had been offered to the local police. He also explained that the search engine has a very clear and strict policy, warning users not to post improper content and alerting them that non-compliance would lead to immediate removal as soon as awareness about violations had been achieved.

On the other hand, it did not appear reasonable to pretend continuous in-advance control with respect to the videos posted on its sharing service, being such monitoring factually impossible given the amount of contributions uploaded by users. He concluded by stating that, while the company was performing every effort to individuate technical means allowing to prevent improper content to be posted, right now the most effective preventive filter appeared to be "community control", as users generally were eager to report the presence of unacceptable videos.

Domestic legal experts questioned the AG's action in the specific case, considering it hardly compatible with general principles set by EU Law as well as by local provisions.

Specifically it's been noted that the EU Directive no. 2000/31 on E-Commerce contained several provisions on providers' liability and explicitly exempted providers a general obligation of controlling Internet content.

Considering the search engine's prompt reaction in the specific case, it appeared truly difficult to understand from which perspective the AG in Milan could find the company's conduct resulting in wrong doing and in a criminal offence.

Various options appear possible, but the following two seem to be those most likely to explain the AG's position:

- either the intention was to achieve an exact idea about how posts are placed by users on the portal's video sharing service and about the technical proceedings involved when content is uploaded,
- or the background of the action had to be found in a recent judgment issued by a first instance Court<sup>43</sup>, which – while dealing with defamatory content posted on a blog – established that a blog owner's liability had to be considered equal to that of an editor in chief of a newspaper (being the AG's idea that of extending the principle to providers).

**10.2.** Politicians perceived the ongoing discussion as an appealing playground for gaining consensus and called for stricter rules, meant to tighten control on Internet content.

One of the arguments brought forward is that currently a disproportion occurs between liability of publishing houses with respect to newspapers' or magazines' content and responsibility of Internet Providers as to web posts.

The Secretary of the Italian Department of Justice called for additional regulation, in order to set 'equal rules' for content liability, unconditional of the media used for content diffusion. He also announced that the Government was planning to look into the problem of proper control of web access by minors as well as into that of violent video games.

Recently a group of local MPs had also expressed serious concern about a "vacuum of legislation", which – they felt - occurred with respect to improper exposure of minors to harmful web content and which they planned to fill through a bill meant: (a) to prevent providers from accepting content submitted by users aged less than fourteen, and (b) to make posting of content by adolescents aged between fourteen and seventeen conditional to parental consent.

In addition, sanctions for non-compliance would be significantly tightened and would involve – in terms of co-liability - minors, their parents and providers (who could face website blocks).

Sounds familiar with what we've heard in the early times of the Internet era. Are we right back to the point where all started from?

## Footnotes

1. Felix Hofer is a founding and naming partner of the law firm Florence (Italy) based law firm Hofer – Loesch – Torricelli; he can be contacted at the following E-mail address: [fhofer@hltlaw.it](mailto:fhofer@hltlaw.it).
2. Reference is to communication means such as SMS, MMS, VOIP, etc.
3. i.e. practices as: spamming, electronic, marketing/advertising on cell phones, pop up ads, banners, profiling through RFID, fidelity cards, cookies, monitoring through audio-visual means, etc.
4. all of them taking part to the so-called "Article 29 Data Protection Working Party – DPWP", set up (by Directive 95/46/EC) as an the independent EU Advisory Body for: "providing expert opinion from member state level to the EU Commission on questions of data protection, promoting harmonized application of the general principles of the Directives in all Member States through co-operation between data protection supervisory authorities, advising the EU Commission on any Community measures affecting the rights and freedoms of natural persons with regard to the processing of personal data and privacy" (so the official description of the DPWP tasks as available at the URL: [http://ec.europa.eu/justice\\_home/fsj/privacy/docs/wpdocs/tasks-art-29\\_en.pdf](http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/tasks-art-29_en.pdf) ).
5. LG (i.e. Landgericht) Berlin.
6. Dated January 14th, 2003.
7. In its decision the Court applied consolidated jurisprudence on unsolicited commercial messages delivered through electronic devices (the decision called specifically on the provisions set by Article 823 of the German Civil Code – BGB and Article 1 of the Unfair Competition Act – UWG).
8. Decision of June 24th, 2002.
9. To explain some effects linked to the introduction of the Euro currency.
10. Dated May 20th, 2002.
11. Reference is to information collected for a specific purpose being used for a different one.
12. CASPIAN (i.e. Consumers Against Supermarket Privacy Invasion and Numbering).
13. i.e., in all 120 countries where the Italian company had a business presence.
14. In its opinion dated May 30th, 2002.
15. In the DPWP's view for companies providing services via the Internet 'place of establishment' means neither the place of location of supporting technology nor the place at which web site is accessible, but the place where the company's business activity is pursued.
16. Are more countries than one involved, compliance with all national laws will result necessary.
17. Unless such equipment is in use only for transit purposes (as back bones, cables, etc.) of telecommunication networks.
18. Not be confused with ownership.
19. e.g. as to the choice of the data's storage, transfer, altering or as to the ways and the purposes of data's collection.
20. Defined as standard part of HTTP traffic, containing any kind of information about a targeted individual (e.g. pages viewed, ads clicked, user ID, etc.).
21. Before cookies' placement on a HD.
22. i.e. software applications sent by a web site to a computer.
23. i.e. software secretly installed in PCs, e.g. when downloading other software, as a music player.
24. Also known also as so-called "E.T. applications", because - once lodged in user's PC - they "phone home" and report about data subject's habits, collect data and send it to another location.
25. On June 28th, 2003.
26. Save the achievement of goals of public interest as protection of minors.
27. Through general blocking or filtering measures.
28. For the 9th Circuit.
29. According to Section 230 of the Communications Decency Act – CDA.
30. Decision August 13th, 2003.
31. OLG (= Oberlandgericht) in Hamburg
32. "Nimm2" (i.e. "Take2").
33. Reference is specifically to Section 14/2, no. 3 of the Trademark Act.
34. Dated February 27th, 2003.
35. Directive 2000/31/EC of the European Parliament and of the Council of June 8th, 2000, on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).
36. Legislative Decree no. 70 dated April 9th, 2003.
37. Neither are they called to investigate actively facts or circumstances indicating illegal acts; on the contrary they're required to report such illegal acts, when acknowledged, to the competent authorities; finally Providers – if requested by authorities - have to comply with instructions for immediate access blocking to illegal content.
38. So Section no. 14.
39. Save when: (i) the transmission of the message originates from the provider itself, (ii) the provider selects the receiver of the message, (iii) the provider selects or modifies the information transmitted.
40. So Section no. 15.
41. So Section no. 16.
42. Save the case when providers become aware of illegal acts conducted or illegal information supplied by its clients and does not remove promptly such content or block access to it.
43. Tribunale in Aosta

*The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.*

Specific Questions relating to this article should be addressed directly to the author.



Do you have a question for the author?

#### **View Related Articles:**

[Deeplinking, Framing And Metatags: The Italian Legal Framework \(Portolano Colella Cavallo Studio Legale\)](#)

[Italian Administrative Court blocks Telecom Italia's High Speed 20Mbit Internet \(Portolano Colella Cavallo Studio Legale\)](#)

[The Italian Communications' Watchdog regulates VoIP services \(Portolano Colella Cavallo Studio Legale\)](#)

[Italian Courts on Betting Sites Black-List \(Portolano Colella Cavallo Studio Legale\)](#)

[Minimum Security Measures For Personal Data Protection \(Trevisan & Cuonzo Avvocati\)](#)

#### **Other Information about Hofer Loesch Torricelli**



[View summary of all information contributed by Hofer Loesch Torricelli](#)



[Most Popular Article in Italy](#)

[Contributor Most Read In Italy](#)