Quaderni di Diritto Mercato Tecnologia

Rivista Scientifica

ISSN (Online edition): 2239-7442

QUADERNI DI

diritto mercato tecnologia

Numero 1
Anno V
Gennaio/Marzo 2015

CON CONTRIBUTI DI:

Alberto Maria Gambino, Davide Borelli Casiere,
Caterina Del Federico, Francesco Saverio Martucci di Scarfizzi,
Marianna Orlandi, Rosaria Petti, Vincenzo Zeno-Zencovich

Intermediary liability. The "Achilles' heel" of the current legislation: the courts. A comparative analysis with the U.S, focusing on copyright infringement

di
Caterina del Federico

Abstract
The topic of this paper regards the uncertainty of the legal framework and the analysis of the majority orientation of the courts with reference to the Internet Service Provider liability on the Web.
A comparative analysis, which focuses on intermediary liability for third party copyright infringement, of Europe and United States, is treated. It is highlighted how important a uniform interpretation of the courts in this field could be.
First a "bird's eye view" on Intermediary liability in the U.S., in comparison with EU legal framework, is outlined.
Secondly, the scope of the "safe harbor" and the "intermediary involvement" through procedures including "notice and take down" are explained.
It is clear how the interpretation of the courts can be considered the "Achilles' heel" of the harmonization with regards to ISPs' liability.
In conclusion the paper tries to identify some possible solutions in order to achieve the harmonization and to make more transparent the legal framework in this field.

L'argomento del presente contributo riguarda l'incertezza del quadro legale e l' analisi del maggiore orientamento delle corti con riferimento alla responsabilità dell'Internet Service Provider sul Web.
Viene effettuata un'analisi, con l' utilizzo dello strumento comparatistico, che si focalizza sulle violazioni del diritto d'autore da parte di terzi, in ambito sia europeo che statunitense. Si evidenzia l'importanza dell'interpretazione fornita dalle corti in tale ambito.
Prima di tutto viene delineata una panoramica sul regime di responsabilità degli intermediari negli Stati Uniti, in comparazione con il quadro normativo europeo.
In secondo luogo vengono illustrati l' esenzione da responsabilità e il coinvolgimento dell' ISP tramite procedure, inclusa quella di "notice and take down".
E' chiaro come l'interpretazione delle corti possa essere considerata il "tallone d' Achille" dell' armonizzazione per quanto concerne la responsabilità dell'ISP.
In conclusione il contributo cerca di individuare alcune soluzioni possibili per raggiungere l' armonizzazione e per rendere più chiaro il quadro legale in materia di responsabilità dell' ISP.

scope of the “safe harbor”. -5. The “intermediary involvement”. -6. Beyond the “safe harbor”: a grey area? -7.The “Achilles’ heel” of the harmonization: the courts. -8.Conclusions.

1. Introduction.

The Internet is a massive global communication complex with an unprecedented ability to bring people and information together from all over the world in a global marketplace of ideas, goods, and services.
Not surprisingly, the Internet phenomenon has been described as “The third Industrial Revolution” [1], especially considering its impact all over the world. Indeed, the Internet represents, beyond doubt, the biggest innovation in the world of the communication.
The Internet is a means of great transformation of the contemporary society and it is configured not just as a model of the network organization, but also as a new form of expression for individuals and community.
The expansion of Internet capabilities entails political, social and even legal implications. This is because more people, more commerce online and more services affect the growth of contract disputes and Internet torts, since more people interact online.
The transnational nature of the Net [2] and the massive global diffusion of messages, images, video and any other type of communication that can be placed on Web pages, create difficulties in identifying the individuals responsible for the offenses committed on the Net.
Thus, the problem of the concrete identification of the offender arises. It is precisely in this scenario that the Internet Service Provider appears. The question is whether it is possible to configure, a responsibility on the Internet Service Provider, besides the responsibility of the “real author”.
The ISP is an entity which performs business activity on the Network. This activity is based on providing services that are considered typical of the information society services.
It is clear that the Internet Service Provider plays a crucial role in enabling people around the world to communicate with each other. Indeed, without the ISPs, there would be no access to the Internet and to the affluence of information that we are able to access just at the click of a mouse.
Moreover, without social media, blogging platforms and newsgroups, the Internet users would lose a valuable way of publishing their opinions and instantaneously sharing information. But because of their technical capabilities, the ISPs are under an increasing pressure to act as “gatekeepers” of the Internet from governments and interest groups.
One of the major issues within the affirmation and the increasing development of the Internet is therefore to define ISPs liability. One of the problems of these years is to clarify the extra contractual liability in which the ISPs incur in relation to telematic torts.
Thus, the most controversial issue in this field concerns the liability regime to be applied to ISP’s business activities in the case of violations committed (by a third party) using the services that the ISPs offer to their users.

In order to resolve these issues, the Community legislator has provided with the 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" (E- Commerce Directive). Indeed, it contains some provisions, specifically devoted to govern the matter of Internet Service Provider liability (articles 12-15).
The E-Commerce Directive was transposed within Italy with the Legislative Decree n. 70/2003. In both the regulations the level of the ISP liability depends on the activity carried out by the ISP. This liability regime establishes the conditions, in negative, to which the ISPs cannot be held liable for violations, damages and torts committed by third parties on the Net in which the ISP provides its services.
From the entire framework emerges, on one hand, the lack of transparency and the non clear-cut regime of the norms. On the other, the interpretation given by the courts "does not shine for crystalline clarity" since even in front of a similar norm the orientations could be very different.
In confirmation of this statement, this present paper provides a brief comparative analysis of the U.S. Digital Millennium Copyright Act and the E-Commerce Directive, focusing on copyright infringements. This is for two reasons.
First of all, in order to make unquestionable that Internet is a borderless technology and for this reason it requires a clear regulation to be as harmonized as possible, also at the international level. Indeed, any uncertainty of the legal framework which governs online activities causes damages to the functioning and the growth of global e-commerce and to the borderless digital technology.
Secondly, in order to prove that one of the first steps for the harmonization would be a uniform interpretation among the courts.

2. A "bird's eye view" on Internet intermediary liability in the U.S.

The most considerable reference in identifying the different types of intermediaries is the United States Digital Millennium Copyright Act of 1998 [3], precisely the section 512 [4]. Indeed, this section contains detailed rules for the limitation of intermediary liability in the field of copyright infringements.
Such rules permit to the Internet Service Provider to be exempted from liability, in certain cases and under certain circumstances. These exemptions represent the so-called "safe harbors".
Nevertheless, according to the DMCA, to be eligible under any safe harbor, a party must satisfy three basic requirements. First of all the party has to be qualified as a 'service provider'. Then, the party has to adopt, reasonably implement and to inform its users inherently to the policy which provides for the termination of 'repeat infringers' accounts. Lastly, the intermediary must accommodate and not interfere with the 'standard technical measures' that are applied by the copyright owners in order to identify and to protect their works.

As regards to the first requirement, the party has to be qualified as a 'service provider' in the specific meaning of the section 512(k), which contains two different definitions of Internet Service Provider.
The first definition applies to benefit of the safe harbor in relation to the transitory communication. It defines the ISP in a strict meaning:

> "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received".

Conversely, the second definition is applied in order to take advantages of the other safe harbors and it considers the ISP in a very broad way:

> "a provider of online services or network access, or the operator of facilities thereof".

Anyway, to benefit from the "safe harbor" an internet intermediary must fall within the category of the different models of intermediation covered by the DMCA. This latter contained several types of service intermediaries.
The first is the so-called 'communication conduits', in section 512(a). This norm covers the most passive category of intermediaries, those offering "transitory digital Network communications". This definition comprises any activity of:

> "transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections".

The analyzed rule confirms an exemption from the civil liability for user-generated content, providing that such activity is initiated by the user and directed to the designed recipient. This activity must take place through an automated process without any modification or selection of the content of the recipient, and without copying the material.
Then, the material has to be made available in a manner which is ordinarily accessible to anyone other than the anticipated recipient, and it cannot be maintained longer than necessary.
All this means that the ISP in question shall not be liable for its activity if it does not initiate the transmission or select the material and the recipients of the material. Moreover, the intermediary does not retain copies of the material longer than necessary for the purpose of carrying out the transmission and it does not modify the content of the material that has been transmitted [5].

Section 512 (b) considers a second category of 'conduit activity system', that of 'caching'. This genre of activity consists of:

> "intermediate and temporary storage of material on a system or Network."

The activity in question is undertaken by the ISP for the purpose of enabling subsequent users to access material that has been made available by one particular user, i.e. the "cacher". Briefly, the intermediary acts in order to make the information more readily and effectively available to the Internet users. But, the conditions that have to be fulfilled by the service provider in order to benefit from the 'safe harbor' are several.
In this present case the intermediary shall not be the originator of the content, nor modify or select the content. It shall act as an intermediary between the provider of the disputed content, i.e. the content provider, and the user of the content in question, i.e. the user.
In addition, the ISP shall comply with any "return technology" designed by the content provider where such technology meets some certain requirements. Thus, the intermediary shall also keep to the access restrictions set by the content provider itself.
The last condition to be fulfilled is that of the obligation to respond expeditiously to any infringement notice with the removal or disabling access to the infringing material.
The ISP must act, once it has been informed that such material has been removed from the originating site or that it will be removed in pursuant to a court order. With regard to this last condition, it is clear that, once a notification of a claim of copyright infringement over the cached materials is received by the ISP, this latter must expeditiously act to remove or to disable the access to the material claimed to be infringing.
In any case, the notification has to include a certain acknowledgment of the intermediary. It can be the acknowledgment that the material has previously been removed from the originating site, or that the access to it has been disabled, or the case in which a court has ordered the removal of such material.
The second category of intermediary is that of 'content hosts'. Under section 512 (c) different types of storage activity which occur are provided:

> "at the direction of a user of material which resides on a system of Network controlled or operated by or for the service provider" [6].

The Internet Service Provider in question benefits from the 'safe harbor' if it does not have the actual knowledge [7] of the infringing nature of the material, and if not aware of facts or circumstances from which the infringing activity is evident.
Anyway, once the intermediary has obtained such knowledge or awareness, it must act expeditiously to remove, or disable access to the alleged infringing material.

In addition, the intermediary must not receive any financial benefit directly attributable and connected to the infringing activity. In case the service provider has the right and the ability to control such activity, as well as get notified of claimed infringement, it must respond expeditiously to remove, or disable the access.
There is a further restriction for this category of intermediary. Indeed, it also must have a designated agent for the notification of claims of infringements and it must follow the special procedure of notice and take-down [8].
Moreover, for what concerns the procedure, the section 512(c)(3) clarifies which requirements the notification should contain to be effective and the section 512(f) and 512(g) provide certain safeguards in order to avoid the effect of possible erroneous or fraudulent notifications or counter-notifications.
That of 'search service and application service providers' is the type of intermediary described under the section 512(d). It is provided the immunity for the intermediary activity of:

> "information location tools, including a directory, index, reference, pointer, or hypertext link".

These services are different from that of 'hosting' because they also facilitate the access to the content, but they do not necessarily host it. The conditions to be fulfilled by the service provider are those contained in the section 512(c).
The last category of intermediary provided by the Digital Millennium Copyright Act is that of 'non profit educational institutions', described by the section 512(e) as intermediary which acts as service provider for their staff [9].
It is stated that if the members of the institution commit infringing actions, these activities cannot be attributed to the institutions concerned.
But, in any case, the institution has to provide to all users of its system or network informational materials that accurately describe and promote compliance with US copyright law [10]. There is a particularly significant rule in Section 47 U.S.C. 230 [11].
It is a general norm which gives complete immunity for "good faith editorial choices" to any provider and user of an interactive computer service for information created or developed by another person or entity.
Contrary to the DMCA, this rule refers to a broad definition of intermediary, it considers "interactive computer service" as:

> "any information service, system or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions" [12].

The last relevant norm in order to make a categorization of the different models of intermediaries within U.S. is under the section 32(2) of the Lanham Act [13]. It protects the publishers of a periodical or electronic communication which are considered "innocent infringers and innocent violators" from damages and certain injunctions for contributor trademark infringement [14].
In this case the safe harbor also includes the limitation of the possibility to act for a claim in order to obtain an injunctive relief in circumstances in which an injunction would interfere with the normal operation of the online publisher [15].
The result is that the U.S. legal framework, in identifying the different categories of intermediary, can be easily led to litigation abuses. Indeed, the norm contained in the Lanham Act could cause the abstention of intermediaries from exercising editorial discretion in doubtful situations, with the purpose of not falling outside the copyright safe harbor [16].
The confusion can be clearly perceived since the plaintiff has the possibility to attribute the same model of acting as either a general tort claim, or a more specific copyright or trademark claim.

3. A comparison with the EU legal framework.

In order to benefit from the exemptions provided by the E-Commerce Directive, a party has to be qualified as 'service provider' providing 'intermediary services'. The Internet Service Provider is defined in the Directive as:

> "any natural or legal person providing an information society service" which is defined as: "any Information Society service, that is to say, any service normally provided for remuneration [17], at a distance, by electronic means and at the individual request of a recipient of services" [18].

Thus, comparing the Directive with the DMCA, the object results to be quite different. Indeed, the object of the European E-Commerce Directive is not limited to the field of copyright, but it devotes four articles (12-15) to the regime of liability of "information society service providers" [19].
Just like the DMCA, the E-Commerce Directive adopts a functional definition of 'Internet Service Provider'.
This subject is qualified through the functions which itself is supposed to carry out ('mere conduit', 'caching' or 'hosting') and the way they are supposed to act ("normally for remuneration", "at a distance", "by electronic means" and "at the request of a user"). Indeed, the specific conditions for eligibility under each exemption of liability provided by the European Directive are strongly inspired by the U.S. DMCA which entered in force few years earlier.
Differently from the DMCA, the E-commerce Directive does not provide any general requirement, such as adopting a "termination policy" or

accommodating with ‘standard technical measures’. It is considered just the mere requirement of being an “intermediary service provider”.
On the other hand the European Directive is narrower than the DMCA. Thus, the Directive requests in all the cases that the service in question has to be provided at the individual request of the recipient, thus excluding TV broadcasting and radio. Moreover, the Directive rules out those services which are provided entirely at distance. By contrary, these kind of services are expressly considered in the U.S. Digital Millennium Copyright Act.
Specifically, in order to give a definition of the Internet Providers within Europe, articles 12,13, and 14 can be considered. The first one refers mainly to the 'Internet access providers' and other providers of technical services. Article 12 of the Directive identifies the activity of “mere conduit” as :

> “the transmission in a communication network of information provided by a recipient of the service, or the provision to ace to a communication network”.

The requirements to benefit from the safe harbor are those of the DMCA. The problems arise in considering the lack of definition regarding the ‘communication network’ and the uncertainty over whether filters would be considered to select or modify the content [20].
Article 13 regards the activity of ‘caching’ and its definition is very similar to that given by the DMCA. In order to benefit from the safe harbor it is required that the provider:

> “does not modify the content and complies with the rules regarding the updating of the information and the conditions. It must not interfere with the lawful use of technology to obtain data on the use of the information”.

This latter point is less clear in comparison with the U.S. DMCA.
In case of receiving notification aimed at the removal of the cached material from the network, or at disabling access to the material, or the ordering by a court or an administrative authority, the intermediary must act expeditiously to do so. But, in the DMCA just the court can give such an order.
The last article 14 concerns ‘hosting’ provider. The hosting activity can be defined as:

> “the storage of information provided at the request of a recipient of the service”.

Here, in order to benefit from the immunity the Internet Service Provider does not have actual knowledge of the illegal (either civil or criminal) activity or information, nor (as regards claims for damages) have awareness of facts and circumstances from which such illegality is uncontroversial.
At this point, once the intermediary has obtained such knowledge or awareness, he must act expeditiously in order to remove or disable the

access to the information. Anyway, the hosting provider, according to the norm, does not have the authority or the control over the recipient. Thus, it is not clear how the Internet Service Provider can be able to act. Indeed, this is probably the most controversial safe harbor of the Directive.
Moreover, it does not specify the meaning of "actual knowledge", and properly because of this lack EU Member States have adopted different approaches in the implementation of this norm of the Directive [21]. Then, it has to be considered that the extent to which the activities of the intermediary should consist of hosting is not clear. Thus, on this point the courts within Member States use to give different interpretations.
By contrary to the DMCA [22], which prescribes it separately and specifically, in the Directive there is no specific provision that covers the conduct of providers of information location tools. The result within Europe is that the Member States are inclined to adopt diverging approaches to their liability [23].
In addition, the E-Commerce Directive does not formally deny a service provider from any exemption of liability as a result of receiving a "benefit directly attributable to the activity".
However, on this point, the domestic courts in Europe have regularly referred to this (non-legal) criterion. Thus, denying hosting intermediaries from the safe harbor [24], especially in French case law. On the other hand, the domestic law and the case law within Europe have added a similar practical requirement so that the general rules regulating Internet intermediaries liability in Europe and US are in a very similar legal framework.
Like the DMCA, a hosting provider under E-Commerce Directive will not be liable for third party infringements, unless it did not expeditiously act in order to remove or to disable the access to such content or activity, upon obtaining knowledge of their infringing character [25].
And, following section 512(m)(1), also article 15 of the Directive forbids the Member States to impose on Internet intermediaries a general obligation to monitor third party content, or actively track facts or circumstances indicating the illegal activity. Thus, leaving the ISPs in a mere passive role.
It is worth to emphasize that the E-Commerce Directive does not create a real common liability regime for all the Member States, whereas it only constitutes additional liability exemptions.
In the light of this, there could be different liability regimes within Europe [26].

4. The scope of the "safe harbor".

The aim of the DMCA and the European Directive is substantially the same, namely that of limiting Internet Intermediaries liability in order to encourage the growth of the digital economy [27]. The major differences arise with regard to the statutory approach and to the procedural rules [28].
The first clear difference is that while the European Directive adopts a "horizontal" approach, dealing with liability of Internet intermediaries in

general, in the United States different regimes of liability in relation to different kinds of content are provided.
Then, while the DMCA is a federal statute which is directly enforceable, the E-Commerce Directive just gives a common legal framework that Member States must implement in their domestic legislation.
Indeed, the competence to choose the procedural rules within Europe, as stated in the Directive itself, is given to the Member States. In order to define the exemption from liability under the safe harbors, it has to be pointed about that the liability can be of three different types. The civil liability in the sense of monetary damages, excluding the injunctive relief [29]. The exemption for this type of civil liability is contained in the section 230 of the Communication Decency Act.
Then, there is a type of civil liability which can also include certain forms of injunctive relief. It is important to recognize the possibility for the courts to order a service provider to help to stop infringements. But, on the other hand it is also of significant importance preventing the imposition of an excessive "weight" on the Internet intermediaries. The use of injunctions is for these reasons controversial. Thus, several legislations, like section 512 of the DMCA, limit and condition the use of such injunctions. In fact, in the 17 U.S.C. sec. 512(j)(2) are listed the factors that have to be considered by the courts in applying injunctions [30].
The DMCA is even clearer since it also provides for two different types of rules for injunctions depending on whether considering an intermediary performing 'mere conduit activity', or if it has to be taken into account the type of activity listed in the section 512(b, c, d, e) [31]. By contrast, the situation within Europe is more complicated. On one hand, it is true that there is an exemption from the general obligation to monitor. But, as mentioned above, on the other hand the Member States are allowed to use injunctions in their own national legislation.
In this way they are able to impose on the intermediary the obligation of notification of the illegal activity or the identification of the users. Indeed, art. 15.2 of the Directive clearly provides that:

> "Member States may establish obligations for information society service providers prompt to inform the competent of alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements".

In addition to one of the other two types of liability explained, there is the criminal one. This model is followed by the majority of the EU Member States using the discretion left by the Directive in the extend safe harbor to the criminal liability. But it has also to be noted that the requirement of the "actual knowledge" demands more than a generic knowledge or awareness to be satisfied for purposes of criminal intent.

Indeed, an intermediary will escape from the criminal liability in the absence of a very clear evidence of intent to participate in the illegal activity [32].

5. The "intermediary involvement".

A report of the Organization for Economic Co-operation and Development identifies four types of systems which are used in the cooperation between intermediaries and law enforcement.
The first that has to be considered is that of "Notice and take down" (NTD). This system is the one which is used by the US and its discipline is contained in section 512 of the DMCA. It requires hosting companies to act expeditiously in removing content which is claimed to be illegal, once they receive the notice of the illegality of the content itself. It is also required to nominate an agent for the reception of the notification.
Moreover the claimant has to specify with a self-certification that he has the authority to pursue the claim and that the information in the notification is accurate.
Section 512(g) confers the intermediaries immunity:

> "for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent".

This kind of immunity is specific for editorial choices. This statement means that an intermediary can be considered liable for not having offered sufficient protection to the right holders. But, at the same time it cannot be held liable for not having removed or disabled access to the content of Internet users.
Thus, in order to benefit from the immunity, the intermediary has to follow some additional steps. Firstly, it must take reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material. Once it receives a counter-notification described in paragraph (3), it must promptly provide the person who provided the notification under subsection (c)(1)(c) with a copy of the counter-notification.
Then, it has to inform that person that it will replace the removed material or cease disabling access to it in 10 business days. The last step to fulfill is the one of replacing the removed material and ceasing disabling access to it. The time factor is crucial, not less than 10, nor more than 14 business days following receipt of the counter-notice. This is unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network [33].
The problem is that the requested material is taken down for a period of time which may be significant, in this way interfering with the free speech. Then, it is not clear whether the copyright owners are required before making their takedown request to consider fair use which is designed to ensure the

balance between copyright exclusivity and public interest. Concluding on this system it is even weird that claimants only need to make a statement with regard to the legitimacy of their claims.
By contrast, the defendants must do that under oath for purposes of counter-notice, risking in this way the consequent penalties for perjury and civil damages that can be imposed. In Europe there is not a uniform procedure, even if some EU countries have adopted a specific one. A particularly unclear point within EU, is the significance of "actual knowledge" to which correspond the duty to act for the removal or for the disabling.
This uncertainty is evident in the Recital 48 [34] of the E-Commerce Directive according to which the Member States may require hosts to:

> "apply duties of care, which can reasonably be expected [...], in order to detect and prevent certain types of illegal activities".

The lack of clarity of this provision creates not only "grey areas" for the activity of the internet intermediaries, but also a glaring inequality within Member States. Moreover it can be considered as a potential threat especially in relation to the development of the European single market as regards to the electronic communications [35]. The danger of such procedures is in the difficult balance of interests between public and private interests.
Another procedure is that of 'notice and notice' (NN). It represents a very simple mechanism which requires an intermediary to send on the alleged infringer the notice received by the right holder. The peculiarity of this system is that it creates a self-regulatory initiative in the absence of state-controlled procedure.
The advantage is that it allows individuals to take down content effectively and rapidly, without spending time for court proceedings. This system is the one adopted, e.g. in the Defamation Act of the UK [36], and most used in Canada [37].
Also important is the notice and disconnection procedure (ND). The aim of this system is to shout out the so called "repeat infringers" using a system of graduated response. The sanctions comprised in this procedure depend on the extent of recidivism of the alleged infringer. The first notice will be merely informative and contains several steps in the case of the repetition of the infringing activity within a specific period of time up to the termination of the Internet connection.
This system was adopted in the French HADOPI law where it culminated with the imposition of a sanction of suspension of Internet access and was administrated by an administrative authority without any judicial participation. Thus the French Constitutional Court found it in violation with the principles of freedom of expression, presumption of innocence and to the due process [38].
It can be found a similar system also in UK's Digital Economy Act, which requires the ISPs to provide copyright owners, upon request, with anonymized reports which permits the copyright owners to apply for a court order [39].

This act also provides for the feature introduction of a graduated response scheme through a code of practice administrated by OFCOM, the UK's communication regulator.
With regard to the filtering and monitoring operations on the material there are some controversial points that have to be noted. In the DMCA, the imposition to monitor is clearly limited by section 512(m) [40] that states that the condition to respect in order to benefit from the safe harbor cannot require "monitoring or affirmatively seeking facts indicating infringing activity".
At the same time it has to be analyzed the section 512(i) of the DMCA regarding conditions for eligibility. The limitations on liability established by this section shall apply to a service provider only if the service provider has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers.
Moreover the service provider must accommodate and not interfere with standard technical measures. As stated, "standard technical measures" means technical measures that are used by copyright owners in order to identify or to protect copyrighted works that have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process.
These measures have to be made available to any person on reasonable and non-discriminatory terms, and they do not impose substantial costs on service providers or substantial burdens on their systems or networks.
From these rules emerges that, with the accordance of the "multi-industry standard process", can be imposed on the ISP a certain degree of filtering and monitoring. Consequently, there is the possibility to emit an injunction with regard to mere conduits. Thus, derogating to the prohibition of section 512(m). Whatever, section 512(j) lays out the considerations that courts should consider in order to the injunction relief [41], limiting the judiciary's discretion.
The EU Directive states that the service provider has "no general obligation to monitor" under article 15. But, at the same time the 12.3 gives the possibility for a court to require the ISP to prevent an infringement. Thus giving a particularly wide discretion to the European courts [42].
Briefly, it can be affirmed that both the DMCA and the EU directive contain the prohibition of the "general obligation to monitor", but both allude to the possibility of requiring the installation of filters for illegal content.

6. Beyond the "safe harbor": a "grey" area?

As explained above, in order to be included under the regime of DMCA and the EU directive several requirements have to be satisfied. Thus, not all the intermediaries can benefit from this special regime of liability since they do not fall in the categories provided in the legislative framework. As a rule, the

normal liability for copyright infringements is evaluated by the laws or the case law relating to the territory within the action has been brought.
Generally, in the European law these rules are mainly laid down by copyright law or tort rules, while in the US common law tradition such liability is governed by common law rules [43]. Between the end of the '80s and the '90s U.S. and Europe tried harmonizing their IP laws in order to combat counterfeiting in a more effective way. Indeed copyright is governed by uniform and harmonized rules in Europe and in the United States [44], which provide for a common standard of protection in the field of copyright [45].
Among them are particularly significant the Berne Convention and the WIPO Copyright Treaty which provide for a universal threshold standard of protection [46]. The first contains rules regarding the author's exclusive right to authorize the public communication, reproduction, adaptation, arrangement, translation, public performance, and/or broadcasting of his work [47]. The second adds the copyright owner's exclusive right to "make available" and "authorize any communication" of his work to the public [48].
Very similar [49] rights are also recognized in the EU Copyright Directive and in the United States Copyright Act [50]. Both in Europe and in the United States, a plaintiff claiming direct copyright infringement has to prove that it has ownership of a valid copyright. Thus the right holder must show that his works are original and fixed in a tangible medium of expression. Furthermore it has to prove a violation of one of the exclusive rights he was granted over his work. With the Internet growth, new issues have arisen, particularly in relation to the intermediary liability for third party content.
Both courts tried to determine whether the unauthorized display and making available work on the Internet could be considered a violation of the author's exclusive right in the case in which the ISP merely gives access to such content. The courts agree in considering that any unauthorized diffusion of a copyrighted content is a violation of the author's exclusive rights of reproduction.
Much more problematic is the indirect liability for third party infringing. First of all, it is more common that an intermediary is involved in indirect liability than in direct. Indeed it happens very often that an ISP: assists, is involved, encourages, controls and/or benefits from a third party infringing activity.
Consequently, theories related to contributory infringement and vicarious infringement have been developed both in Europe and in the United States.
Moreover, the U.S. common law has recognized that, under certain circumstances, one who has not directly infringed a copyrighted work, but has contributed to, or encouraged the infringement, may be liable for "contributory infringement" [51].
According to this doctrine, the plaintiff has to prove a direct infringement by a third party and the actual or constructive knowledge of this infringement by the alleged contributory infringer. Lastly it has to prove that the alleged contributory infringer induced, caused or materially contributed to the infringing activity. Only through showing this proof the plaintiff can prevail in a contributory infringement claim.

Within Europe there are no provisions regarding the contributory copyright infringement. At the same time, several EU Member States provide in their legislations some rules which entail civil or criminal liability on the subject that encourages, assists or benefits from another person's tort.
All of this is based on the theories of "indirect liability", which has had great success so far before the European courts [52]. Mainly, these theories require the plaintiff to prove an infringement by the direct transgressor and some kind of assistance and the knowledge of the infringing activity by the intermediary.
For what concerns the doctrine of vicarious liability, this theory also has its roots in tort law, but it did not have the same success of contributory liability. It provides that, under certain circumstances, one can be liable for the torts committed by another person because of the specific relationship he has with the transgressor.
The leading case on which this doctrine was set up is "Shapiro Bernstein & Co. v. H.L. Green Co" [53]. In this present case the Second Circuit specifically states that a party may be liable in the sense of vicarious liability for copyright infringement if it has the right and ability to control the infringer's act, and if it receives a direct financial benefit from the infringing activities.
By contrary to the contributory liability doctrine, vicarious liability does not require any knowledge or involvement in the infringing activity, but a control on it. Within the european tradition the equivalent of vicarious liability is the concept of "liability for the acts of others". Unlike its common law equivalent, it has to be generally stated in statutory provisions, limited and expressly provided by the law. For this reason it did not have success in the context of EU courts.

7. The "Achilles' heel" of the harmonization: the courts.

Both the DMCA and the E-commerce Directive "hosting" safe harbor state that a hosting service provider can be liable for third party content only if it has actual knowledge or sufficient awareness of its illicit character, and it did not act expeditiously to remove or block this content after obtaining such knowledge.
Moreover, section 512 (c)(1)(B) adds two conditions according to which the service provider may also be liable if having the right and ability to control the activity and if it financially benefitted from the infringing activity.
Both these conditions are not provided in the E-Commerce Directive, but at the same time they are taken into consideration within the European courts. Therefore the requirements are very similar. The problem is that of the interpretation by the courts.
The "knowledge standard" is one of the requirements which results in differing interpretations before the U.S. and the EU courts. This lack of clarity within the courts creates considerable problems. As pointed out above, the crucial inquiry in order to determine the Internet intermediary liability is significant in determining whether the intermediary had knowledge of such infringing activity.

Both the DMCA and the EU Directive specify that the "knowledge standard" is the actual knowledge of the illicit content or activity, or the awareness of facts and circumstances from which the infringing activity is apparent.
In the United States, the knowledge standard under the DMCA includes actual knowledge, or sufficient awareness of facts and circumstances from which the infringing activity is apparent. The second part of the knowledge standard, the awareness, would require the service provider to take action any time he is aware of a "red flag" which means "aware of any circumstances from which infringement would have been apparent" for a reasonable person. This is according to a Senate Report on the DMCA [54].
Hence, the requirement of the actual knowledge is normally satisfied by receiving an appropriate notification from the right holder and sufficient awareness should be satisfied by any other information which may constitute a "red flag" of infringement. Thus, the tendency of the U.S. courts is generally to require a high standard of "sufficient awareness" – as close as possible to that of actual knowledge.
The landmark case in this field is "Viacom v. Youtube" [55], in which Viacom sued Youtube alleging that this letter had engaged in massive copyright infringements. Viacom allows its users to upload and view hundreds of thousand of videos owned by Viacom itself without any permission. The Southern district of New York stated that in order to lose the benefit of the hosting exemption, it should have had knowledge of a specific and identifiable infringement of particular individual items.
Moreover, the court added that the service provider's alleged general knowledge that the infringement is omnipresent did not impose on him a duty to monitor or to search the service for infringements. Further, the court found that Youtube does not have the "right and ability to control" infringing activity because:
"there is no evidence that Youtube induced its users to submit infringing videos, provided users with detailed instructions about what content to upload or edited their content, prescreened submissions for quality, steered users to infringing
videos, or otherwise interacted with infringing users to a point where it might be said to have participated in their infringing activity" [56].
Then, an appeal begun, but one week before the parties had to appear before the court, a settlement was reached stating that no money changed hands. Thus, it is clear that red flag exists where a service provider subjectively knows facts that would make a specific instance of infringement objectively obvious to a reasonable person.
Under these standards, neither the actual nor the red flag knowledge standards are met when a defendant has only general knowledge that its services could be used to host and view infringing content. By contrast, the European courts have broadly interpreted the requirement of actual knowledge standard under the E-Commerce Directive.
Indeed, in the case "Twentieth Century Fox et al. v. British Telecommunications (BT) PLC" [57], the U.K. High Court found sufficient that the service provider (BT) had general knowledge that their services were

being used to infringe copyright in general to order to BT to block its users from accessing to the file-sharing site.
Thus the court did not consider any specific knowledge [58]. Similarly, in the case "Society des Auteurs des arts visuals et de l'Image Fixe (SAIF) v. Google" [59]. In this present case the Paris Court of Appeal states that the sole awareness by the service provider that its service may be used for copyright infringements does not imply its liability.
Moreover, Google was ready to "de-index" such content upon the notification of the information which enabled for identifying and then localizing the infringing contents. In both the regulatory frameworks [60], in order to avoid liability, a service provider, once obtaining knowledge of infringing content or activity, should act to remove or disable the access to the infringing material.
At the same time in the lack of specific knowledge, the service provider cannot be bound by any general obligation to monitor. Also here, in the interpretation of the courts, there is a huge discrepancy. With regards to the U.S., this criteria is generally followed by the courts. This is clear in the case "UMG Recordings, Inc. v. Shelter" [61], in which the ninth circuit upheld the Californian Central District's opinion.
The District court stated that the Internet intermediary in the present case is protected under the DMCA, establishing that a service provider is:

> "entitled to broad protection against copyright infringing liability so long as it diligently removes infringing material upon notice of infringement".

Indeed, the United States Court of Appeal states that in the case of absence of specific knowledge of a particular infringing activity, a video sharing platform had no duty to monitor or seek out copyright infringement.
By contrast, the situation within the European courts is much more controversial. As stated on several occasions by the European Court of Justice, it is true that Member States are prohibited to impose any general obligation to monitor on the service provider. But, on the other hand, Member States can impose on the service provider specific injunctions under the national legislation. This is in accordance with the recitals of the Directive [62], article 11 of the Enforcement Directive [63] and the article 8(3) of the Copyright Directive [64].
In "Twentieth Century Fox et al. v. British Telecommunications (BT) PLS" the U.K. the High Court ordered that main U.K. ISPs block some of their users from accessing a content sharing platform where most of the content was unauthorized.
The same happens in the case "Youtube v. SPPF" [65], in which the Paris TGI held that hosting providers had the duty to implement all reasonable means to prevent the recurrence of content already notified as infringing.
The tendency is that in general the European courts consider the adequate response to awareness of infringing activity to be added of monitoring already notified infringing material. The sole action of taking down content

upon notification of their infringing character is not enough. In conclusion, even if the legal framework concerning ISPs liability is more than similar in Europe and in the United States, the courts interpreted this in a widely different way, thus rendering inadequate protection for those involved and creating uncertainty [66].

8. Conclusions.

At the end of this paper it is appropriate to make some comments. It has been explained that Internet has global implications. It has been shown how important the involvement of the Internet Service Provider in the Internet world is, as well as the increasing pressure that this subject is receiving.
Even if there are some specific rules, called "safe harbor", which have the aim to exempt the Internet Service Provider from liability, under certain circumstances. Despite some significant and positive changes in this field, it appears obvious which the tendency of the case law is. The one to held the ISP responsible.
It has been almost fifteen years since the introduction of the European Directive, and yet, there are still some grey areas on this field. It has been explained how the Directive was introduced to encourage the development and the growth of e-commerce, defining in a precise manner ISP's safe harbors. Nowadays the needs and the interests appear to be changed.
There is a clear redefinition of the role of the Internet Service Provider and the courts represent the first place in which the changed social needs are collected. Today the necessity is no longer one of Network growing, but, maybe, of rethinking the legislative framework, as well as the allocation of responsibility, at this stage of the Internet. The lack of uniformity of the decisions given by the courts imposes a duty on the lawyer: the duty to reflect on the relevance and the actuality of the Legislative Decree 70/2003 for the Italian lawyers and of the E- Commerce Directive for those within Europe.
Indeed, the technical evolution of the global network has now exceeded the definition of the Internet Service Provider given by the Directive.
The latter subject, at the time of the Directive, was totally unrelated in respect to the information stored. Furthermore, the services offered today by the ISPs are not even comparable to those of the early 2000s. As an example the figure of the 'active hosting' category of ISP does not emerge from any legal regulation [67] within Europe. Such a change in the object of the services provided by the 'hosting provider' symbolizes a development of these subjects: the development of new forms of content aggregation. These are those digital platforms fed by the materials uploaded by the users [68]. Consequently, the use of such content aggregators postulates the use of system of indexing, categorization, selection and organization by the Internet Service Provider which in this way becomes 'active hosting'.
The problem is to technically define how the provider intervenes on this material, thus losing its neutral role. The risk of these uncertainties is to

cause an intimidatory effect against the Internet Service Provider. Another category not defined by the Directive is that of the 'search engines'. They facilitate the finding of data through the myriad of pages in the World Wide Web, consequently enhancing the ability of individuals to receive and to communicate information.
Therefore, more certainty would be desirable. Another controversial point is that of imposing on the ISP, on its own initiative, once aware of the illegality of the content, the disabling of the access or the removal of the illegal content. The articles 16 and 17 do not admit this hypothesis. It happens in the practice, even if, according to the rules, the task to disable the access must be received from an administrative or judicial authority. This shows the discrepancy between the provisions of the Directive and the praxis.
Moreover the procedure of "notice and action" is unclear, because it is not defined neither the time, nor the modality with which the obligation is triggered on the provider. The obligation is to inform the judicial or the administrative authority having supervisory functions, once the provider is aware of alleged illegal activities. Indeed, neither the Directive nor the Legislative Decree provide criteria to ensure that the provider was effectively aware of illegal content placed on the Web by its users.
By contrary, a specific procedure of "notice and take down" is adopted in the U.S. It would be appropriate to introduce a defined procedure of notice and take down also in the EU. Firstly because it would realize a harmonization within Europe, giving higher certainty. Secondly it would also represent an instrument in order to balance different interests. On one hand the intermediaries interests, and on the other the interest of the victims of the illicit content.
It is therefore desirable that the European legislator revises the Directive 2000/31 in order to introduce a harmonized procedure of "notice and take down" and also new rules of liability with regard to search engines and the new categories of 'hosting providers'.
The aim is to clarify some essential functionalities which have now become strictly inherent to the activities of the new 'hosting providers'. Thus, creating a uniform guide for the allocation of responsibility on the Internet service provider.
A new intervention would be also necessary in order to clarify the boundaries of the neutral role of the ISP, the basis to benefit from the "safe harbor". The reason of such interventions is the continuous technological growth. This leads to a new balance involving: the interest of the right holders in having efficient remedies against the infringement of their right, the interest of intermediaries to continue to run their business in the most efficient way and the interest of the Internet users to utilize services permitted by the law.
Moreover, a fair balance between fundamental rights such as the freedom of communication and expression and the right to privacy has to be considered.
The need to innovate the Directive is confirmed in two public consultations proposed by the EU Commission between 2010 and 2012, aimed to evaluate the implementation of the Directive, in accordance with its article 21.

These are: the “Public consultation on the future of electronic commerce in the internal market and the implementation of the Directive on electronic commerce” and the “Public consultations procedures for notifying and acting on illegal content hosted by online intermediaries”.
The consultations did not lead to an effective revision of the legislation in the analyzed field. Indeed, the Directive has been considered sufficient. However, it was recognized that some application in order to enhance its application would be appropriate.
Given the global nature of the Internet and considering that what happens on the Web has side effects which exceed the territorial boundaries, a minimum standard of harmonization at the international level would also be desirable. It would be possible especially with regards those countries which have a globally consistent legal framework.
Beyond the legal framework, the task of interpreting the law, and especially to close the loopholes of the legislation, is reserved to the courts. These play a fundamental role in giving consistent guidelines within an increasingly global market.
If the courts interpret differently the same norm, regulation or principle in this field, the result is inadequate protection for everyone. It represents a big deal of legal insecurity for right holders, Internet intermediaries and users in the digital environment and, also, it increases the tension between the conflicting interests.
In the light of what has been stated, as most often happens in the word of the law, there is not a clear-cut solution. Only an integrated and consistent effort would clarify the actual role of the ISP and their responsibility regime.
A first step could be, undoubtedly, a review of the European Legislation in this field. A law dating back to fifteen years ago cannot be expected to be applied to a world continuously evolving. Then, the task to achieve the harmonization, not just within Europe, but also at the International level, as much as possible, is down to the courts. This, surely would increase legal certainty. Moreover, considering the continuing evolution of Internet it would be appropriate a greater use of soft law as integration instrument.
Cooperation between main stakeholders would be helpful, as the Organization for Economic Co-operation and Development also states between 2010 and 2011. Indeed the OECD states that governments may choose to cooperate with the main stakeholders in order to identify the appropriate circumstances under which Internet intermediaries could take steps to educate users, assist rights holders in enforcing their rights or reduce illegal content. At the same time minimizing burdens on intermediaries and ensuring legal certainty for them.
Lastly, given the importance of the Digital Economy, which represents the background on which the ISP acts, one of the primary step to achieve the harmonization also in the field of intermediary liability could be, at the european level, to create a Digital Single Market.
This is demonstrated by one of the last press releases of the European Commission, that on the Digital Single Market Strategy, 25 March 2015 [69]. The latter has been followed by the Communication on Digital Single Market

Strategy for Europe, 6 May 2015 [70]. As the President of the European Commission announced "By creating a connected digital single market, we can generate up to EUR 250 billion of additional growth in Europe in the course of the mandate the next Commission […]".
The Communication contains and explains the three main pillars on which the Digital Single Market will be built. First of all, a better access for consumers and business to online goods and services across Europe has to be achieved. Secondly, the right conditions for digital networks and services to flourish have to be created [71]. Then, the growth potential of our European Digital Economy needs to be maximized.
The goal il clearly to transform the European society and ensure that it can face the future with confidence, in close cooperation with all relevant stakeholders.
All this together would probably lead to a fair balance of the various interests involved and to the much sought legal certainty.

Note:

[*] Il presente contributo è stato preventivamente sottoposto a referaggio anonimo affidato ad un componente del Comitato di Referee secondo il Regolamento adottato da questa Rivista.
[1] B. L. Smith, The third Industrial Revolution: Law and Policy for the Internet, in Recueil des Cours, 2000 (282), 229 et seq.
[2] See U. Draetta, Internet nel diritto internazionale, in G. Finocchiaro, F. Delfini (edited by), Diritto dell'informatica, 2014.
[3] DMCA, 1998, available at: http://www.copyright.gov/legislation/dmca.pdf. The Digital Millennium Copyright Act implements two 1996 World Intellectual Property Organization (WIPO) treaties: the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty.
[4] Section 512 of the DMCA derives from the Online Copyright Infringement Liability Limitation Act (OCILLA), which is a federal law creating a conditional 'safe harbor' for online service providers shielding them from liability for infringing acts committed by others. OCILLA was passed as a part of the DMCA and is also called 'the safe harbor provision' or 'DMCA sec. 512'.
[5] 17 U.S.C. sec. 512 (a) (1998).
[6] This would include, e.g., clouds computing services or simple email storage.
[7] I.e. is not aware of facts or circumstances from which the infringing activity is apparent.
[8] The procedure of notice and take-down is contained in section 5125(g).
[9] Such as faculty members and graduate students performing teaching or researching within the university.
[10] The inclusion into the safe harbor of these kind of activities gives the educational institutions greater certainty. Its inclusion in the safe harbor is not taken for granted. Indeed, by contrast, online activities provided by public educational institutions are explicitly excluded from the scope of the

EU Electronic Commerce Directive of 2000, since this is applicable only in relation to information society service providers and information society service required to be "normally provided for remuneration".
[11] Section 230 of the Communication Decency Act (DCA) of 1996 is a landmark piece of the Internet legislation in the United States, codified at 47 of the U.S. Code.: "protection for private blocking and screening of offensive material". Available at: http:// www.law.cornell.edu/uscode/text/47/230.
[12] Cf. Section 230(f)(2) and (3).
[13] The Lanham act, enacted July 5, 1946, is codified at 15U.S.C. sec. 105. It represents the primary federal trademark law in the United States. Available at: http://www.co-lumbia.edu/~mr2651/ecommerce3/1st/Statutes/Lanham.pdf.
[14] Cf. Title 15 U.S.C., sec. 1114(2)(B).
[15] Cf. Title 15 U.S.C., sec. 1114(2)(C).
[16] Lemley M., Rationalizing safe Harbors in Journal of Telecommunications and High Technology Law 6, 2007, p.101-103. The Author writes: "The inconsistent treatment of different types of claims also leads to litigation abuses by plaintiffs who seek to recast claims subject to significant immunity as different types of claims with lesser or nonexistent immunity. I will give just two examples[...].This sort of gamesmanship is undesirable.
[17] Recital 18 of the E-Commerce Directive clarifies that the notion of "remuneration" does not mean that the services shall necessary be given in exchange for a fee, so long as they can be qualified as part of an "economic activity". Thus, recital 19 states that this is not the case, e.g., for governmental services and public education.
[18] Article 1 of the Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations. Available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31998L0048.
[19] Cf. art. 2(a) of the European E-Commerce Directive 2000/31, referring to the definition in art. 1(2) of the Directive 98/34, as emended by the Directive 98/48.
[20] EU Commission, EU study on the Legal analysis of a Single Market for the Information Society. New rules for a new age? 6. Liability of online intermediaries (Brussels: EU Commission, 2009), 14 http://ec.europa.eu/information_society/newsroom/ cf/dae/itemdetail.cfm?item_id=7022.
[21] In Spain it was required a formal notification by the competent administrative authorities. In Finland was considered the fulfillment of a notice and take down procedure. In Germany the national courts determined on a case by case basis.
[22] Cf. 17 U.S.C. sec. 512(d).
[23] In Austria, e.g., it was extended the protection of "mere conduits" ex art. 12 of the Directive. In Spain, Portugal and Hungary it was explicitly extended the protection of article 14.

[24] See, e.g., Paris Court of Appeal Sep. 3, 2010, "eBay Inc et al. v. Parfums Christian Dior et al" (prec.) (holding eBay liable for third party's infringing offers as a result of eBay's active role in "the promotion and orientation of such offers so that they may lead to an effective sale on which eBay will reap a percentage fee"). See also Cour de Cassation, Jan. 14, 2010, "Telecom Italia v. Dargaud Lombard and Lucky Comics "(holding Tiscali liable as a result of displaying (paying) advertising next to the infringing content); Cour de Cassation, Oct. 21, 2008, "Sedo v. Hotels Meridien et al." (holding Sedo liable notably as a result of the commission reaped on the sale of infringing domain name); Cour de Cassation, Oct. 21, 2008 "Lafesse v. Myspace" (denying hosting exemption to Myspace because it reaped benefit from advertisement placed on the website every time the infringing video was seen). But see Cour de Cassation, Feb. 2, 2011, "Nord Ouest Production et al. v. Dailymotion" (prec.) (holding that advertising fees were irrelevant since it did not involve a control over the information).
[25] Cf. Council Directive 2000/31/EC, art. 14.
[26] Van Eecke P. and Truyens M., Liability of online intermediaries in Legal analysis of a Single Market for the Information Society, (SMART 2007/0037), study of European Commission, available at: http://ec.europa.eu/digital-agenda/en/news/legal- analysis-single-market-information-society-smart-20070037, p.27.
[27] See S. REP. No 105-190, at 1-2 (1998) ([the DMCA is] "designed to facilitate the robust development and word wide expansion of electronic commerce, communication, research, development and education in the digital age". And, as regards to the EU, see the Proposal for the European Parliament and Council Directive on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p.3.
[28] Cf. 17 U.S.C. sec. 512(c)(3) and (g), in which the DMCA provides specific notification and counter-notification procedures. See also 17 U.S.C.(h)(2), which regards a simplified procedure to enable the right holder to identify in an easy way direct infringers by filling out a subpoena before a federal court.
[29] Injunctive relief refers to the obtaining of a court order, an injunction, which consists of a prohibition of an act or a condition. The prohibition can be applicable to all future conduct of the recipient, or, most commonly, limited to a predominated period of time.
[30] Cf. 17 U.S.C. sec. 512(j)(2), Considerations. The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network; (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement; (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to non infringing material at other online locations; and (D) whether other less burdensome and

comparably effective means of preventing or restraining access to the infringing material are available.
[31] In the first case a court can grant injunctions only in one or both of the following forms: "(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order. (ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States." See: U.S.C. Section 512(j)(1)(B). For all the other safe harbors, the following injunctive relief is available: "(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network. (ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order. (iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose." See: U.S.C. Section 512(j)(1)(A).
[32] Indeed some EU member states (such as Italy and Germany) explicitly distinguish actual knowledge, which can impose on the intermediary criminal purpose, and mere awareness which links to civil liability.
[33] Cf. 17 U.S.C. sec. 512(g)(2).
[34] Recital 48, Directive 2000/31/EC: "This Directive does not affect the possibility for Member States of requiring service providers, who host information provided by recipients of their service, 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".
[35] Indeed, a higher standard of care imposed in a Member State may hamper the operation of a national service provider, giving advantages to the competitors in other member states. In this sense the German Federal Court of Justice (Bundesgerichtshof) held in several cases that eBay, having knowledge of the fact that a particular seller had infringed trademark law, was found responsible for not having taken measures to prevent further infringements, if such measures were possible and economically reasonable. See: "Rolex v. E-bay/Ricardo", BGH 11.03.2004, I ZR 304/401.
[36] Cf. sec. 5 of the Defamation Act, 2013. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/269138/defamation-guidance.pdf.
[37] The Canadian Association of Internet Service Providers, the Canadian Cable Television Association, and the Canadian Recording Industry Association agreed in 2000 to a voluntarily "notice and notice" system.
[38] See note 60 supra.

[39] Moreover the DEA provides for a dispute resolution mechanism requiring both substantial user involvement and an effective appeals mechanism.
[40] Cf. 17 U.S.C. sec. 512 (m): Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on— (1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or (2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.
[41] Cf. 17 U.S.C. sec.512(j): (iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.
[42] There are several recent cases in EU, inherently the issue of filtering and monitory obligation. See: "Pirate bay", in which the Belgian Court orders two ISPs to block the website, available at: https://edri.org/edrigramnumber10-1dutch-isps-block-piratebay/, (last visited 31.1.2015). See also: "BREIN v. Ziggo/XS4ALL", where a Dutch court orders two ISPs to block Pirate Bay, (The Hague District Court case 374634/HA ZA 10-3184, Jan. 11, 2012).
[43] Seagull Haiyan Song, A Comparative Copyright Analysis of ISP Liability in China Versus the United States and Europe, Selected works in The Computer & Internet, 2010, available at: http://works.bepress.com/seagull_song/2.
[44] The Berne Convention for the Protection of Literary and Artistic Works (1886), to which the U.S. adhered in 1989. Available on WIPO Database of Intellectual Property Legislative Texts. The Universal Copyright Convention (UCC) (1952). The WIPO Copyright Treaty (WCT), Geneva, (1996). The Agreement on Trade-Related aspects of Intellectual Property Rights, Annex 1C of the Marrakesh Agreement Establishing the World Trade Organization, Marrakesh, Marocco, 1994.
[45] As regards to a specific harmonization within Europe on copyright, see van Gompel S., van Eechoud M.M.M., Guibault L., Helberger N., Hugenholtz P.B., Harmonizing European Copyright Law: The Challenges of Better Lawmak, in Information Law Series, nr. 19, Alphen aan den Rijn: Kluwer Law International 2009. And for more certainty in the fields of copyright see van Gompel S., Formalities in copyright law, An analysis of their history, Rationales and Possible Feature, 2011.
[46] These International conventions also provide a common threshold condition to the availability of any exception which should: (i) be limited to certain special cases, (ii) not conflict with a normal exploitation of the work, and (iii) not unreasonably prejudice the legitimate interests of the author. These threshold requirements are known as the three-step test and they are contained in art. 9(2) of the Berne Convention, art. 13,17 of the TRIPS Agreement, art. 10 of the WIPO Copyright Treaty and art. 16 of the WIPO Performances and Phonograms Treaty. The three-step test is of primary importance and "the courts have to identify individual use privileges case-by-case and the three-step test can serve as a source of inspiration for national

law makers seeking to institute flexible exceptions and limitation", see Geiger C., Gervais D., Senftleben M., The Three-Step Test Revisited: How to Use the Test's Flexibility in National Copyright Law, available at: http://ssrn.com/abstract=2356619.
[47] Cf. Berne Convention, 1971 Paris Text, Art. 8,9 (I), 11, 11(bis), 12,14.
[48] Cf. WIPO Copyright Treaty, 1996, art. 6,8.
[49] EC Council Directive 2001/29/EC On the harmonization of certain aspects of copyright and related rights in the information society, see art. 3: "right of communication to the public of works and right of making available to the public". See also chapter II of EC Council Directive 2001/29/EC providing the exclusive right of the author to authorize or prohibit the reproduction (art.2), Communication and making available to the public (art. 3) and Distribution (art. 4) of his work.
[50] Cf. U.S. Copyright Act, sec. 106.
[51] It has to be noted that the Copyright Act and the Lanham Act do not impose liability on anyone if not on the direct infringers.
[52] EWHC, Feb. 20, 2012, "Dramatico Entertainment Ltd & others v. British Sky Broadcasting Ltd & others". In this judgment The Pirate Bay was held liable for "authorizing" copyright infringement by its users.
[53] "Shapiro, Bernstein & Co. v. H.L. Green Co.", 316 F. 2d 304 (second Cir. 1963).
[54] See S. REP 105-190, p. 44,45. "[...]However, if the service provider becomes aware of a ''red flag'' from which infringing activity is apparent, it will lose the limitation of liability if it takes no action. The ''red flag'' test has both a subjective and an objective element. In determining whether the service provider was aware of a ''red flag,'' the subjective awareness of the service provider of the facts or circumstances in question must be determined. However, in deciding whether those facts or circumstances constitute a ''red flag''—in other words, whether infringing activity would have been apparent to a reasonable person operating under the same or similar circumstances—an objective standard should be used.
[55] "Viacom International Inc et. al. v.YouTube", 718 F. Supp. 2d 514 (S.D.N.Y. 2010).
[56] See Case 1:07-cv-02103-LLS, U.S. (S.D.N.Y.), available at: https://www.docketalarm.- com.
[57] "Twentieth Century Fox et al. v. British Telecommunications PLC", (hereinafter TCF v. BT) U.K. High Court July 28, 2011.
[58] By contrast, in the case "Societé des Auteurs des arts visuels et de l'Image Fixe (SAIF) v. Google", (Paris Cour d' Appel, Jan. 26, 2011), the Paris Court of appeal held that the sole awareness by a service provider that its service may be used for copyright infringement did not entail its liability since it had shown to be willing to de-index the infringing images, upon notification of the information enabling their identification and localization. The court states "The mere fact that the defendants are aware that the automatic indexation is likely to infringe copyrighted work is not sufficient to entail their liability since they are ready to "de-index" such content".

[59] Paris Cour d' Appel, Jan. 26, 2011, Society des auteurs des arts visuels et de l'image fixe (SAIF) v. Google France, SARL and Google Inc.
[60] Cf. 17 U.S.C. sec. 512(c)(1)(A)(iii) and art. 14(1)(b) of the Directive 2000/31/EC.
[61] "UMG Recordings, Inc. v. Shelter Capital Partners LLC", 667 F.3d 1022 (9th Cir. 2011).
[62] See Recital (45) and (47) of Council Directive 2000/31/EC. (45) "The limitations of liability of intermediary service providers established in this Directive do not affect the possibility of injunctions of different kinds; such injunctions can in particular consist of orders by court or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information or the disabling of access to it." (47) "Member States are prevented from imposing a monitoring obligation on service providers only with respect to obligations of a general nature; this does not concern monitoring obligations in a specific case and, in particular, does not affect orders by national authorities in accordance with national legislations".
[63] Cf. Recital 23-24, art. 3 and art. 11 of Council Directive 2004/48, on the Enforcement of Intellectual Property Rights.
[64] See Article 8 (3) of Council Directive 2001/29/EC of the European Parliament and of the Council of 22 may 2001 on the Harmonization Of Certain Aspects Of Copyright And Related Rights In The Information Society. "Member State shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right".
[65] "Youtube v. SPPF", TGI Paris, Apr. 28, 2011.
[66] See Béatrice Martinet Farano, Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches, TTLF Working Paper No. 14, available in: http://www.law.stanford.edu/programs-and-centers, transatlantic-technology-law-forum, -working-paper-series.
[67] This category is indeed created from the case law, e.g. the judgment of the case Google - Vividown and RTI-Italia On line.
[68] It refers to the so-called Used General Content, e.g. Google, Youtube and the social networks.
[69] The document is available at:http://europa.eu/rapid/press-release_IP-15-4653_en.htm.
[70] COM(2015) 192 final, available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf.
[71] This second point also contains the provision of combatting illegal content on the Internet involving the Internet Intermediary Service Providers. It is stated "The principle, enshrined in the e-Commerce Directive, that Internet intermediary service providers should not be liable for the content that they transmit, store or host, as long as they act in a strictly passive manner has underpinned the development of the Internet in Europe. At the same time when illegal content is identified, whether it be information related to illegal activities such as terrorism/child pornography or

information that infringes the property rights of others (e.g. copyright), intermediaries should take effective action to remove it. Today the disabling of access to and the removal of illegal content by providers of hosting services can be slow and complicated, while content that is actually legal can be taken down erroneously. 52.7% of stakeholders say that action against illegal content is often ineffective and lacks transparency. Differences in national practices can impede enforcement (with a detrimental effect on the fight against online crime) and undermine confidence in the online world. As the amount of digital content available on the Internet grows, current arrangements are likely to be increasingly tested. It is not always easy to define the limits on what intermediaries can do with the content that they transmit, store or host before losing the possibility to benefit from the exemptions from liability set out in the e-Commerce Directive. Recent events have added to the public debate on whether to enhance the overall level of protection from illegal material on the Internet. In tandem with its assessment of online platforms, the Commission will analyze the need for new measures to tackle illegal content on the Internet, with due regard to their impact on the fundamental right to freedom of expression and information, such as rigorous procedures for removing illegal content while avoiding the take down of legal content, and whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems – a duty of care".

QUADERNI DI
DIRITTO MERCATO TECNOLOGIA

Numero 1 - 2015
Anno V
www. dimt. it

ISSN (Online edition): 2239-7442