Website blocking injunctions under Swiss law. From civil and administrative injunctions to criminal seizure or forfeiture

Benhamou, Yaniv

YANIV BENHAMOU

WEBSITE BLOCKING INJUNCTIONS UNDER SWISS LAW

From civil and administrative injunctions to criminal seizure or forfeiture

Website blocking is an important issue for legal professionals and courts in Switzerland [1]. It is a measure that consists of blocking a website, a web page or a specific content, which may be ordered by an authority against a service provider [2] (e.g. Swisscom may be ordered to block access to certain websites containing defamatory texts or works that infringe copyright).

1. INTRODUCTION

From a technical point of view, *hosting providers* can generally *withdraw specific content* available on their portals [3], whilst Internet service providers (ISP) can only block a domain name by *blocking the IP or DNS address [4]. Blocking IP addresses* consists of *blocking access to a server* with a specific IP address. This type of measure entails blocking all of the offers included on the server and not just the web page with the illegal content. *Blocking DNS addresses* consists of *blocking the process that makes it possible to translate* an IP address into a domain name (the name by which an IP address is commonly known) [5]. For financial and practical reasons, DNS blocking is most often used. This may be performed by means of software that can answer a DNS request, either directly (because the service provider recognises the URL) or indirectly (by consulting the register in question). The user who wished to access the blocked site will be redirected to a page indicating that the site is blocked or does not exist, as the software will not provide them with the requested IP address [6]. These measures are only partially effective as they are relatively easy to by-pass. Users can *by-pass* DNS blocking by entering the IP address or by using another DNS server and by-passing the blocking of the IP address by connecting to the destination server via an intermediary server (proxy server). Furthermore, many blocked websites are stored in full on other servers by mirroring or caching [7]. There is also a risk of *overblocking*, i.e. when not only the infringing content is blocked on the IP address, but also other (legal) contents that are available on the same IP address [8].

From a legal standpoint, there is currently *no specific rule or clear case law.* Swiss copyright law (LDA) is under review and is subject to a draft law (pLDA) [9], but the final draft will certainly not provide for any blocking measure with regard to ISPs [10]. The pLDA is also limited to copyright, whereas the portals cover all types of infringement (e.g. privacy, data protection, breach of copyright, trademark law). Such a measure may be envisaged in private law as part of an injunction, of a criminal seizure or forfeiture, or administrative proceedings with regard to certain content. Although such a measure may be effective, or even essential in preventing access to some content online, particularly when the hosting provider or content provider is located in another country [11], it is subject to shifting case law and various controversies. It must be brought up to date.

YANIV BENHAMOU, PHD, ATTORNEY AT LAW, LECTURER UNIVERSITY OF GENEVA, GENEVA, YANIV.BENHAMOU@UNIGE.CH

2. PRIVATE LAW: LOCKING IP AND DNS ADDRESSES

Today, there is *no specific legal basis* or (civil) case law authorising the blocking of IP and DNS addresses [12]. Such a measure could however be envisaged under the terms of an injunction. The claimant could ask the judge to order the *blocking of an IP/DNS address by ISPs* (and/or the *take down of specific content by the hosting provider*). Such a *blocking could then be ordered* by a judge, without necessarily being qualified as a blocking injunction, for example by ordering the service provider to remove any means of accessing the content. Such a measure must however follow the principle of proportionality [13].

2.1 Capability of being sued in the event of infringing personality rights. As opposed to laws in the United States [14] and the European Union [15], Swiss law has *no specific rules* regarding the civil liability of service providers. Liability is therefore based on *general rules.* This situation should remain unchanged (with the exception of copy-

right)[16]. The service provider's *civil liability* could be incurred if its participation is sufficient to be deemed to have the capability to be sued. The difficulty then lies in determining the *degree of participation,* as any service provider could be considered to be a participant.

In the event of *infringing personality rights* (e. g. invasion of privacy or the violation of honour), the claimant may request an injunction against any participant (CC 28 al. 1)[17]. A *minor contribution* is sufficient. The Swiss Supreme Court allowed the liability of the *Tribune de Genève* as the host of a blog on the grounds that it is possible to take action against *"whosoever has objectively played [...] a role – albeit secondary – in the creation or the development of the infringement"*[18]. The capability to be sued for media providers is therefore *broadly* allowed by the Swiss Supreme Court[19]. Applied to ISPs, this approach would make it possible to *systematically take action* against service providers as they play an objective, albeit secondary, role in transmission of information. The liability is not however unlimited as it must be restricted by proportionality[20].

"As opposed to laws in the United States and the European Union, Swiss law has no specific rules regarding the civil liability of service providers."

2.2 Capability of being sued in the event of infringing intellectual property rights. In the event of *infringing intellectual property rights* (copyright, trademark, patent, design), the claimant may also request an injunction against the participant in the infringement (Swiss International Patents Act (LBI) 66 let. d; Swiss Design Act (LDes) 9 al. 2; Swiss Copyright Act (LDA) 62 al. 1; Swiss Trademarks Act (LPM) 55). It is not clear if the capability of being sued applies in the same manner or less broadly than for personality rights. Case law and doctrine tend to limit the capability of being sued to *qualified participatory acts* with reference to the *patents and design rights rules* (LBI 66 let. d; LDes 9 al. 2) providing for the capability of being sued against any person who incites, collaborates, encourages or facilitates the performance of an infringement[21], or with reference to *art. 50 CO* providing for the capability of being sued against whosoever knew or should have known that the services could infringe the right and that the customers effectively infringe the right[22].

2.3. Assessment. When applied to service providers, the capability of being sued in the case of infringement of intellectual property rights means *rejecting the liability of ISPs* due to a lack of incitement or knowledge of the content and *admitting the liability of hosting provider only if it were aware* of the actual infringements (in the event of a prior summons or when the services are provided intentionally in order to infringe the right). This *approach appears dubious to us,* as injunctions are subject to a certain knowledge of the ISP (fault, negligence), a condition which should be onlywanalysed at the stage of monetary claims, which brings us towards a subjectivization of the infringement. In our view, there should be a uniform solution applicable to all kind of infringements, as the service providers and the online portals can infringe all kinds of rights, and as fragmented solutions depending on the right protected would bring confusion and uncertainty to the matter. It should also be admitted that the ISPs play a role, even purely objective and secondary, in the flow of information and thus in the infringements, and their capability to be sued should be admitted systematically. Such capability to be sued must be then analysed in the light of the proportionality.

3. CRIMINAL LAW: PREVENTIVE BLOCKING (SEIZURE ARTICLE 263 OF THE CRIMINAL PROCEDURE CODE, HEREAFTER CPP) OR PERMANENT BLOCKING (FORFEITURE ARTICLE 69 OF THE CRIMINAL CODE HEREAFTER CP)

3.1 The issue: are websites "objects" that can be sequestered/confiscated? In theory, the service provider does not *incur criminal liability* as it is generally unaware of the type of information placed by the content provider[23]. Nor does it appear to incur specific criminal liability of media, as the service provider has no editorial control over the illegal information[24]. Criminal website blocking must therefore be envisaged on other grounds, based on seizure (preventive blocking) or forfeiture (permanent blocking). In either case *the measure is controversial:* it is not based on *any explicit legal provision* but depends on a *broad interpretation* of the procedural provisions regarding the seizure (Article 263 CPP) or substantive provisions regarding the forfeiture of dangerous objects (Article 69 CP)[25], whereas the wording of these provisions *refers expressly to objects* (physical, tangible assets)[26].

3.2 Case law. This controversy *has not prevented the penal authorities from ordering website blocking* based on seizure/forfeiture. Some Cantonal courts have indeed considered that the virtual intangible nature of internet access does not constitute an obstacle to seizure/forfeiture and have *assimilated websites to objects.* The *Cantonal courts* have thereby approved a blocking order on several occasions based on seizure/forfeiture against an ISP based in Switzerland for websites giving access to illegal information. The central argument being that such an interpretation is in line with the spirit of the law (taking into account technical progress) and that it is *proportional* to block access rather than seize the servers since "he who can do more can do less"[27].

The Swiss Supreme Court has not yet clearly ruled on the issue. In a ruling on 19 March 2015 ("Blogger"), the *Swiss Supreme Court rejected a blocking order* for two websites containing defamatory statements that were grounded on Article 69 al. 2 CP and considered that permanent blocking was *comparable to a destruction* as defined by art. 69 al. 2 CP. The Swiss Supreme Court rejected the blocking order on the grounds that it was *against procedural law* (forfeiture as defined by Article 69 al. 2 CP must be ordered by the judge, and not during the investigation phase) and on *substantive law* (the blocking aims to bring an end to a behaviour, not to prevent the use of

or destroy a dangerous object). The Swiss Supreme Court did however *expressly leave unresolved the issue of blocking based on Article 69 al. 1 CP,* limiting itself to returning the case to the lower court for it to consider if the conditions for blocking were fulfilled (severity of the accusations made and the proportionality of the measure that must be restricted to illegal content) [28].

> *"Given the lack of any clear legal basis or a clear position from the Swiss Supreme Court, it should be analysed whether a website can be considered as an 'object' or an 'asset' that can be seized or forfeited."*

3.3 The two possible interpretations. Given the lack of any clear legal basis or a clear position from the Swiss Supreme Court, it should be analysed whether a website can be considered as an *"object"* or an *"asset"* that can be seized or forfeited.

According to a first approach (literal interpretation), the wording of seizure/forfeiture is *limited to tangible "objects"*. Computer data (or the website blocking) as virtual assets are not covered by seizure/forfeiture, nor are they covered by the provisions regarding theft (art. 139 CP) and damage to property (art. 144 CP). *To address computer data, special provisions* had to be drafted, such as unauthorited obtaining of data (art. 143 CP) and damage to data (art. 144bis CP) [29]. If the penal blocking of websites is to be provided for, *the provisions of the CPC* regarding seizure would need to be completed with an *ad hoc* blocking provision or, if we consider that the role of criminal law is to punish a behaviour and not to bring an end to an issue, complete the civil or administrative measures inspired by art. 15 OID and art. 88 et seq. of the Draft Gaming Act (P-LJAr) [30]. Furthermore, the fact that the P-LJar provides a specific legal basis indicates clearly that the possibility of forfeiture/seizure of websites does not exist, and that such a specific provision is needed.

According to a second approach (broad interpretation), computer data (or the blocking of websites) are objects (or assets) covered by seizure/forfeiture. In the "Blogger" ruling, the Swiss Supreme Court *expressly left the issue of art. 69 al. 1 CrC open* by referring the case to the lower court to consider if the conditions for blocking were fulfilled (suspicions and proportionality). In two *recent rulings* on 16 November 2016 ("Facebook" and "Google"), the Swiss Supreme Court allowed that *computer data* from a user account are objects (or assets) *subject to a filing obligation* (Article 265 CPC) based on a ruling assimilating emails to electronic documents (Article 110 al. 4 CrC) and a loophole in the law excluding monitoring measures by telecommunications stations (Article 269 et seq. CPC) for email service providers such as Facebook/Gmail [31].

3.3.1 Assessment. Although we may note the Swiss Supreme Court's reluctance to allow the website blocking due to the lack of a clear legal basis [32], we can also note a *tendency for a broad interpretation of the laws by the courts* to take into account the technological developments. You need only think of the Swiss Supreme Court's "Blogger" ruling (assimilating computer data to objects or assets), and the rulings of the Federal Criminal Court of Switzerland and the Cantonal Court of Vaud (following the principle of "he who can do more can do less" and aiming to take into account the technological developments) [33].

The absence of a legal basis for website blocking is a *shortcoming* in the law. Supposing that the legislator's intention was to exclude website blocking from the general standard (Article 69 CP), even the specific rules for forfeiture exclude website blocking: for example hardcore pornography or the representation of violence (Article 197 al. 6, 135 al. 2 CP) are subject to similar forfeiture rules, i. e. applicable to object (or representations) of the crime [34] as tangible medium [35]. It seems doubtful, or even inconceivable that civil website blocking cannot be ordered also under criminal law, in any case with regard to websites containing hardcore pornography and showing acts of violence [36]. It may be thought that the legislator unintentionally omitted such measures or extending seizure/forfeiture to websites. This shortcoming must be compensated for by the judge [37].

A broad interpretation requires the *following reasoning.* Computer data can be subject to seizure/forfeiture as dangerous objects having been used to commit offences and compromising morals or public order (Article 69 al. 1 CP). The *analogy* between *objects* and *computer data* was confirmed by the Swiss Supreme Court in the "Blogger" ruling assimilating the Gmail/Facebook user account data to an object and a previous ruling assimilating an email to a letter [38]. Computer data can be considered as having *"served to commit offences and endanger morals or public order"* (e. g. holocaust deniers or defamatory words) [39]. The "he who can do more can do less" approach adopted by Cantonal case law and the Federal Criminal Court ultimately seems appropriate as the legal authority could effectively order the seizure/forfeiture of the physical servers (even those abroad, intenrational legal assistance set aside), and choosing to block the website (i. e. a flow of data passing through the ISP's servers) seems proportional.

> *"Although we may note the Swiss Supreme Court's reluctance to allow the website blocking due to the lack of a clear legal basis, we can also note a tendency for a broad interpretation of the laws by the courts to take into account the technological developments."*

The *website blocking appears therefore possible* according to a broad interpretation of seizure/forfeiture to compensate for a true shortcoming in terms of new technologies. This conclusion is however *debatable* from the perspective of the legality of the penalties and the certainty as to the law (as illus-

trated by the unease and the lack of a clear position from the Swiss Supreme Court), and it would be *beneficial* if the legislator could ultimately provide for an *ad hoc* provision for blocking, or administrative measures based on art. 15 OID and art. 88 et seq. P-LJAr.

4. ADMINISTRATIVE LAW: RULING OR COOPERATION IN ORDER TO BLOCK CERTAIN CONTENT

In some cases, the administrative authorities also have the power to block websites.

4.1 Administrative blocking decision (OID, P-LJAr). The *Ordinance on Internet Domains (OID)* allows for the blocking of a *malicious site* by an administrative decision. The "register" [40] must block a domain name in its purview in the event of serious suspicions that the website in question is used to illegally access the critical data of third parties *(phishing)* or to broadcast malicious software *(malware)* (Article 15 al. 1 let. a OID). The measure is first to be requested by a department fighting against cybercrime recognised by OFCOM (Article 15 al. 1 let. b OID) then confirmed by the Federal Police Office (fedpol) that renders an administrative blocking decision (Article 15 al. 4 OID).

> *"The administrative measures are effective, and have borne fruit in some fields, in that they depend on administrative law making it possible for authorities to investigate and act automatically or negotiate with the ISPs."*

The *Draft Gaming Act* (P-LJar) provides for the addition of a new blocking measure. After fruitless negotiations between the main Swiss ISPs and the Federal Gaming Commission, the draft act provides that this Commission can order the *blocking of unauthorised online gaming sites* for which the operator has a registered office in another country. A black-list of unauthorised offers will be regularly updated and sent to the ISPs for blocking and then published officially (Article 84 P-LJAr).

In this regard, we can also refer to the *pLDA* providing a blocking measure by means of a list drawn up by the Swiss Federal Institute of Intellectual Property (IGE) and an administrative decision. This measure may however be removed from the final draft [41].

4.2 Cooperation aimed at blocking certain content (LMSI, SCOCI). The *Swiss Internal Security Law* (LMSI) provides for a possibility of *blocking on a voluntary basis*. The *Federal Office of Police (fedpol)* may recommend that Swiss ISPs block access to websites for which the servers are abroad and which contain *material inciting violence* (e. g. jihadi propaganda) (Article 13 e, ch. 5 LMSI). As remarked by Cottier, this approach codifies the administrative practice regarding blocking that consists of favouring dialogue with the ISPs that are against any legislation, but based on recommendations and voluntary cooperation [42].

Finally we mention the *Swiss Cyber Crime Division (SCOCI),* created at the end of 2001 and answering to fedpol that allows anybody to *report the existence of suspicious websites or content online:* the reported content is subject to an initial examination, then sent to the authorities for criminal proceedings in Switzerland or abroad. SCOCI also trawls the internet looking for illicit content and supports the ISPs in fighting against pornography by providing them with a list of foreign websites offering certain types of pornography.

4.3 Assessment. The administrative measures are effective, and have borne fruit in some fields, in that they depend on administrative law making it possible for authorities to investigate and act automatically or negotiate with the ISPs. The other side of the coin is that they do not take into account the same procedural laws as the civil and criminal law measures and are limited to certain fields, therefore fragmenting the solutions, or causing uncertainty in fields that have no express legal basis.

5. PROPORTIONALITY

A blocking measure must comply with the principle of proportionality, that is to say, the judge must take into account the interested parties who may be impacted by the measure [43]. Proportionality is particularly delicate with regard to service providers in view of the lack of control and influence that they have over the content [44]. An ISP could therefore argue that, in a specific case, it is not reasonable, from a technical point of view, to prevent access to certain content, and that the measure is disproportionate. It must also target only the illegaé content and avoid preventing access to other licit communication (prohibiting *overblocking*).

5.1 Fundamental rights. In the case of blocking, proportionality implies *taking into account the other rights at stake.* Under Swiss law, there is little case law on this issue, with the exception of a few Cantonal criminal rulings that recognise the primacy of public order, honour or secrecy over the financial interest of the ISP in not taking technical control measures or blocking [45]. Given the lack of case law in Switzerland, it is useful to refer to European law [46].

With regard to *the rights of content holders,* in the Pirate Bay ruling the CJEU considered that the transmission of legal information deserved greater protection than the transmission of illegal information [47].

With regard to *the right of ISPs,* in the kino.to ruling the CJEU considered that blocking does not infringe the basic freedom of the ISPs to do business as they *can continue to do business* in spite of a blocking measure. The blocking measure must **not** however oblige the ISP to make *unbearable sacrifices* (difficult and complex technical solutions that hinder business) and must *leave the ISP the choice* of the measure that best matches its resources [48].

As for the *right of users,* it is better to *avoid blocking* sites offering both *legal content* and illegal content *(overblocking).* This argument has not generally been adopted by the courts as the rulings generally concerned sites that were designed mostly to allow for the sharing of illegal files (e. g. The Pirate Bay) [49]. It is however better to take care that the blocking measure is carefully targeted [50].

"As for the right of users, it is better to avoid blocking sites offering both legal content and illegal content (overblocking)."

As for the *right of platform operators,* in the Pirate Bay ruling, the ECHR considered that the criminal conviction of the site operators was a restriction on their freedom of expression, but that such a restriction was justified, in particular due to the fact that the information in question did not benefit from the same level of protection as political debate [51].

5.2 Proportionality with regard to the websites targeted. To comply with the principle of proportionality, the blocking measure must *target websites that host mostly illicit information [52].* To determine which sites should be targeted, we suggest taking *several criteria* into account, such as the quantity of illegal information, the objective pursued by the portal and the type of information (commercial, political or creative).

As for the *quantity of information,* the target must be sites that offer mostly illicit content, as opposed to sites that have essentially licit content and on which only a small amount of illicit information is available [53].

In terms of the *objective pursued* by the portal, we can draw on foreign case law, in particular the American Grokster case and the European Pirate Bay case. In the *Grokster ruling,* the U. S. Supreme Court found contributory infringement for inducement of infringement based on three factors: (i) the operator *attempted to attract the previous users of the Napster network* (by the name of the products, the advertising sent to Napster users and the configuration of the network that was made compatible with Napster), (ii) benefited directly from the infringement of copyright by *selling advertising space* and (iii) it was *aware that the software was used essentially to infringe* copyright (about 90% of the files exchange on the incriminated network were protected by copyright) without taking any action in this regard [54]. In the *ruling on The Pirate Bay,* the CJEU found that the platform operators' aim was to make works available by infringement of copyright (by indexing the torrent files, offering a search engine for the works by genre categories and popularity) and by *making a profit* (via payments from advertising) and they had been *informed of the illicit nature* of many of the files exchanged (by means of blogs and forums available on the platform). Finally, we can draw inspiration from the Canadian law on copyright that defines the act of contributory infringement of platform operators. This contribution is established according to the *promotion* of the activity of making works available by infringement of copyright, the operator's *knowledge* of the illicit exchanges and the *measures taken to prevent* such exchanges, the *revenue* drawn from these illicit exchanges and the economic viability of the platform without the illicit exchanges [55].

As for the *type of information,* based on European case law, we find that data containing copies of copyrighted works are less protected than *information about political debates* [56] and speeches inciting hatred and violence are unprotected [57].

In *summary,* we can consider whether an operator's offer is manifestly illicit and justifies blocking measures depending on the quantity of illicit exchanges, the revenue generated by these illicit exchanges and the incitations to use the services for said illicit exchanges.

5.3 Proportionality with regard to the technique in question. Proportionality also means adapting the measures according to the system used by the ISP (e. g. automated or otherwise) and technological developments [58]. An injunction would for example be disproportionate if it ordered an ISP with automated services to implement *measures that cannot be automated,* and that could therefore lead to a complete shutdown of the ISP's business [59]. The current state of technology would certainly lead the ISPs to implement blocking based mostly on IP or DNS addresses [60]. The *blocking of IP addresses* seems disproportionate for large operators offering access to thousands of different contents (it means blocking all of the offers available on the server, and not just the web page with the illicit content), whilst it seems proportional for illicit offers with their own server or for IP addresses offering only similar illicit content (e. g. racist, pornographic or almost entirely illegal) [61]. The *blocking of DNS* therefore seems more proportional, and it will often be preferred due to the limited costs for the ISPs [62].

«As for the type of information, based on European case law, we find that data containing copies of copyrighted works are less protected than information about political debates and speeches inciting hatred and violence are unprotected.»

5.4 Proportionality in terms of cost. The issue of the cost of the blocking measure is debated in several jurisdictions that generally allow that the ISPs must cover these costs, even if they are not directly liable for the infringements [63].

Under Swiss law, with regard to *blocking websites under criminal law,* the *ISP may claim a reimbursement from the State,* as compensation for the damage caused by the blocking measure (Article 434 CPC) [64]. For *blocking websites under civil law,* the

courts generally put the *costs at the expense of the losing party* (Article 106 al. 1 CPC) but, it can decide against it when the specific circumstances make the distribution of expenses according to the outcome of the case unfair (Article 107 al. 1 let. f CPC). The service provider may attempt to convince the judge to have the claimant bear the costs of implementing the blocking. It will however be subject to the judge's sole discretion, who may refuse on the grounds that such costs are proportional, for example because it is preferable to leave them at the ISP's expense as they can choose the least expensive option, that they have already made a profit from revenue thanks to the illicit content (through the increased number of visitors and/or advertisers), and that a claimant who is found to be right must not bear additional costs for implementation. Finally, costs appear to be limited and not excessive [65].

"Whereas in other countries blocking measures appears to be effective and the main issue is the enforcement and modalities of such measure Switzerland has still no clear legal basis to implement them."

5.5 Subsidiarity of blocking in relation to direct action or de-indexation. According to the principle of subsidiarity, action must be taken directly against the offender or other participants (advertisers, suppliers of payment services or registrars) and, only as a secondary measure, against the ISP with blocking, on the grounds that the former will be closer to the breach than the latter.

The principle of *subsidiarity has been followed by some courts.* In Germany and in Austria, blocking is only allowed when direct action proves impossible (e. g. because the offender cannot be found) or ineffective (e. g. because implementation is too slow or costly) [66]. In Switzerland, this principle has been suggested in the pLDA [67].

The principle of subsidiarity is *open to criticism* as it has *no legal basis* and often makes *blocking ineffective* (servers are often located in jurisdictions that do not offer effective implementation of the rights or implementation that is slow and costly) [68]. Indeed, blocking is necessary exactly because of the situations where it is not possible to act against these operators. These motives explain why the principle has not been followed by the CJEU or most neighbouring jurisdictions. Blocking should therefore be allowed *independently of other possible measures* (or in any case when the other measures appear slow or expensive) and *cumulatively* with other actions, such as requesting de-indexation of the websites [69]. This approach is all the more justified as *de-indexation* is not a clearly established right, in any event with regard to IP rights, and that the websites continue to be accessible even after de-indexation [70].

5.6 Effective implementation: possibility of a workaround. Blocking measures are sometimes criticised as there can be a workaround. Amongst the techniques used to work around the blocking, we can refer to the use of proxies or regularly changing the IP address/URL hosting the contentious website; some ISPs use several domain names and IP addresses that they regularly change according to the blocking measures targeting some specific domain names [71].

This being the case, the blocking may *not necessarily lead to a complete end* of the infringements; the measure need only be *reasonably effective in stopping or preventing* the infringements [72] and, according to several studies, it substantially reduces traffic to the blocked websites (by 70 to 90%) [73]. The fact that there is a means to work around technical measures does not constitute an argument to abandon them. In many fields, it is possible to avoid control measures (e. g. money laundering). In the same manner, for road traffic, it is not unusual for some offenders to avoid being identified. This does not however mean that measures to control financial flows or speed should be abandoned [74].

The legal implementation is therefore an issue for the rights holders and the authorities. To overcome the aforementioned practices (e. g. regularly changing domain names), some courts order *dynamic blocking injunctions.* In the UK and Ireland, blocking covers websites (online location) without referring to a specific domain name/IP address and provides for a mechanism whereby the rights holder can notify the ISPs of any change or new domain name hosting the illegal site so that the ISP can add it to the blocking measure [75]. A Court even recently adopted a live blocking injunction against an illegal streaming broadcast following a case filed by the Premier League Football Association that was only effective during the transmission of the premier league game and only during the season (i. e. from 18 March 2017 to 22 May 2017) [76]. In Australia, although the measure does not provide for a mechanism for notification of new IP addresses/URL, it can be modified to include new addresses. Other jurisdictions do not provide for dynamic injunctions (in particular Argentina, Austria, Finland, France, Italy, or Spain). A change of address requires a new request for blocking with the Court.

«Amongst the techniques used to work around the blocking, we can refer to the use of proxies or regularly changing the IP address/ URL hosting the contentious website.»

Under *Swiss law,* such a *dynamic injunction* seems contrary to procedural law. The claimant must enter pleadings in order, where applicable, to be able to have the same ruling enforced and to allow for forced execution, without necessarily referring to the grounds [77]. We can therefore envisage two solutions: (i) requesting *direct enforcement [78]* and, for each new IP address/URL used by the operator, making a new request, or

(ii) requesting *indirect enforcement,* by presenting a claim to the court for the enforcement along with any useful documents, including a certificate of the enforceable nature of the claim [79].

5.7 Assessment. Proportionality makes it possible to supervise the measure: after having agreed to the legal grounds, on a civil, criminal or administrative basis, the authority responsible for the measure must carefully assess the proportionality of the measure. It must in particular take into account all of the interests at stake that may be affected by the measure [80]. Such an exercise is delicate, not only due to the lack of control and influence over the content for the service providers [81], but also due to the diversity of blocking techniques, the variety of the types of infringements and websites, and the risk of overblocking. In this context, self-regulation (e. g. practical recommendations issued by the different stakeholders, if possible in partnership with and approved by an authority) to offer greater transparency and clarity to the service provider and to be adapted progressively as technologies develop in a lighter manner than a legal basis.

"In addition to legal measures, it would be practical to encourage self-regulation."

6. CONCLUSION

Whereas in other countries blocking measures appears to be effective and the main issue is the enforcement and modalities of such measure (e. g. costs and the dynamic nature of the measure), Switzerland has still *no clear legal basis* to implement them.

Such a measure is *however provided for on different legal grounds,* but is subject to different controversies. *In civil law,* the controversy is the *capability to be sued* of the ISPs. In our opinion, it must be systematically allowed in reference to the case law relating to personality rights. In *criminal law,* the issue is allowing a *broad interpretation of the seizure/forfeiture* measure in spite of a wording limited to objects. Such a broad interpretation seems possible, or even necessary to make up for a real loophole and with regard to technological developments. This conclusion is however *debatable* from the perspective of the legality of the penalties and the certainty as to the law and it would be *beneficial* if the legislator could ultimately provide for an *ad hoc* provision for blocking, or administrative measures based on art. 15 OID and art. 88 et seq. P-LJAr. Such an *ad hoc* provision must be applicable in a wide-ranging manner, without being limited to certain sectors or specific fields. In *administrative law,* some measures allow for blocking and have proven their effectiveness. They are *however limited to certain fields,* leading to a fragmentation of the solutions, or even uncertainty in fields that do not have a clear legal basis.

Such a measure must therefore be clearly allowed on the basis of *general civil and criminal law,* rather than on specific sectoral rules (e. g. pLDA), in order to *avoid the fragmentation of solutions.* Website blocking may involve any types of infringements, and not just copyright or other field. After having allowed such a measure in principle, the judge must assess it in the light of the proportionality that therefore makes it possible to safeguard all of the interests at stake and to avoid any abuse by the claimed rights holders who wish to block any type of content. This contribution also attempts to *offer different solutions,* i. e. firstly to allow the measure based on different grounds, then to give the *applicable criteria for the proportionality* of the measure.

Alternatively or in addition to the blocking measures, *other methods* should also be considered including *de-indexation of websites and/or a "follow the money"* approach, the idea of which is to associate paid services, credit card companies (e. g. PayPal) and online advertising players, in order to make operating pirating websites less lucrative. This follow the money approach is not yet sufficiently mature and must respect all the fundamental rights and interests at stake (including protecting user data), but would certainly be an effective measure [82].

In *addition to legal measures,* it would be practical to encourage *self-regulation.* This would make it possible to offer clarity and *transparency* to the ISPs, and to develop guidelines regarding proportionality and websites considered to be illicit. For example, we can refer to the guidelines issued by the Council of Europe, in collaboration with the European Internet Service Providers Association (EuroISPA), aimed at assisting the ISPs (particularly in terms of proportionality) or the list drawn-up by the Swiss Cyber Crime Division (SCOCI) listing all of the websites that are accessible online that appear to contain child pornography. Self-regulation will ultimately make it *possible to take account of the development of technologies* by recommending a dynamic/changing manner in which blocking measures should be technically implemented by the ISPs.

Notes: 1) This contribution is a short version of a more detailed Article to be published in the collection pi-ip 2017 folllowing a presentation on "Copyright and challenges: challenges in Swiss law" at the annual IP conference hold at the University of Geneva on 22 February 2017. **2)** "Service provider" shall mean here any internet intermediary offering services to its clients (often automated services) with no editorial control over the illegal information, including hosting provider (i. e. offering a storage capacity where the client may store his own content) and internet access provider (i. e. providing an acess to internet via telephone or broadband access). See Report of the Federal Council of 11 December 2015, The Civil Liability of Internet Service Providers, 20, indicating that the boarders between these functions are often porous because there are mixed or specific forms of providers. **3)** Cottier Bertil, Etude comparative sur le blocage, le filtrage et le retrait de contenus illégaux sur internet, Etude du Conseil de l'Europe préparée par l'Institut suisse de droit comparé, Lausanne 2015, 681 ss; Report (n. 2), 46. **4)** Report (n. 2), 20, 46, indicates that sometimes the hosting provider cannot remove isolated content on a leased server, but only suspens the entire leased server. **5)** Report (n. 2), 47, comparing the deletion of someone's phone number in a phone book. **6)** Equey David, La responsabilité pénale des fournisseurs de services internet, Stämpfli 2016, 339. **7)** Equey, 332, indicating that

there are various open-access DNS resolvers (e.g. Google Public DNS, OpenDNS or French Data Network). **8)** Cf. Equey, 331, indicating that these measures may also lead to performance problems (e.g. slowdown effects or interruptions in the provider's infrastructure for addresses which would not be covered by the blocking measure). **9)** Draft law of the Federal Act on Copyright and Related Rights (Copyright Act, CopA) of 11 December 2015, based on the recommandations of the Working group on Copyright (AGUR12). **10)** AGUR 12 II, statement made to the media on 2 March 217, Modernization of Copyright: compromise solution in the AGUR12 II ("Les propositions de compromis n'incluent pas les mesures prévoyant le blocage par les fournisseurs d'accès, ni l'envoi de messages d'information en cas de violations graves de droits d'auteur par le biais de réseaux pair-à-pair"). **11)** Various web sites allow to geo-locate domain names, e.g. http://fr.geoipview.com. **12)** The situation could change since a website blocking injunction requested by the film distributor (Praesenz-Film) against Swisscom before the Bern Court (Handelsgericht), cf. Tagesanzeiger 15 March 2017, Ein Filmverleih zerrt die Swisscom vor Gericht. **13)** Infra 5. **14)** 17 U.S.C. §512. **15)** Directive 2000/31/CE (Directive E-Commerce) (art. 12–15); Directive 2001/29/CE (InfoSoc) (art. 8 al. 3); Directive 2004/48/CE (art. 11). **16)** Report (n. 2), 3 concluding that no new rule shall be adopted ("Il faut donc renoncer a priori à l'introduction d'un instrument supplémentaire relevant du droit civil") and the same day the need to adopt new rules for copyright in the Federal Council's explanatory Report of 11 December 2015 on the modernization of Copyright, 31 ("Le droit d'auteur constitue une exception. Pour lutter efficacement contre le piratage, il est nécessaire de se doter de réglementations spécifiques"). **17)** One can imagine an infringement of the data protection act (e.g. users of a social network display someone's personal data. Capability to be sued in the event of infringing personality rights apply also in this respect due to the reference of art. 15 al. 1 to art. 28 CC, cf. Rapport (n. 2), 35. **18)** Decision of the Swiss Supreme Court (TF) 5A_792/2011 of 14 January 2013, c. 6.2–6.3. Scholars have criticised this decision because it leads to an unlimited capability to be sued, Schoch/Schüepp, Jusletter of 13 May 2012, n° 36. See however, TF, 6 May 2015, 5A_658/2014, sic! 2015, 571, c. 4.1 "Carl Hirschmann", denying the status of participant of whosever posts on his website a general link to the website of a journal or a radio station because the link is "not specific enough". **19)** Judgment of the Swiss Supreme Court 5P.308/2003 of 28 October 2003, c. 2.5 (website owner who reproduced news articles containing infringements of personality rights); ATF 106 II 92 (journal which reproduced news readers); ATF 126 III 161 (printing company which participated in the diffusion of defamatory articles). **20)** Infra 5. However see Aebi-Müller Regina E., Personenbezogene Informationen im System des zivilrechtlichen Persönlichkeitsschutzes, Berne 2005, N 140; Geiser Thomas, Zivilrechtliche Fragen des Kommunikationsrechts, medialex 1996, 203 ss, 204, considering that liability is also limited by the causation principle between the infringement and the participation of the provider. The infringement should be also promoted in general by the participation and the claimant should evidence the previsbility of the infringement. Rosenthal David, Aktuelle Anwaltspraxis 2013, 727 s: admitting the capability to be sued of hosting provider but not necessarily for ISP due to the lack of causation. Contra: Rigamonti, considering that the causation seems to be always fullfilled as the services of the provider are generally capable "depending on the course of events and general experience of like" to lead to the infringement. **21)** Hess-Blumer Andri, Teilnahmehandlungen im Immaterialgüterrecht unter zivilrechtlichen Aspekten, sic! 2003, 100 s.; Schoch Nik/Schüepp Michael, Provider-Haftung "de près ou de loin"?, in: Jusletter of 13 May 2012, 27 ss, applying the rules of patent and design law to copyright infringements base on the argument that the legislator intended a legislation as uniform as possible for the whole field of intellectual property. He refuses to apply the capability to be sued with reference to CC 28 on the ground that intellectual property relates to commercial good, while CC 28 relates to personality good and its infringement requires a balance of right. **22)** ATF 129 III 588, considering that the rules provided in art. 66, let. d, LBI are similar to those in art. 50 CO. **23)** However see Equey, 250, indicating the provider's position of guarantor ("position de garant") which could lead to the criminal liability as accomplice. See also Swiss Supreme Court, 1B_242/2009, of 21 October 2009: in a judgment of 2 April 2003 of the Cantonal Court of Valais, not officially published, the Court considered that the internet access was not an object subject to seizure/forteiture. The Court however held that the ISP should be informed that they may be accomplice if they do not proceed with the website blocking. **24)** See however Cottier, 690, indicating that platform operatos have generally a certain control over the content and could be considered as a periodical media, even if the Supreme Court has refused to apply CPC 266 so far (measures applicable to periodical media) to a social media operator. Swiss Supreme Court, 4 Mai 2011, 5A_790/2010, c. 5.2; Swiss Supreme Court, 10 October 2013, 1C_335/2013. **25)** Cottier, 684. **26)** See Favre/Pellet/Stoudmann, art. 69 N 1.12; C. Schwarzenegger, Sperrverfügungen gegen Access-Provider – über die Zulässigkeit polizeilicher Gefahrenabwehr durch Sperranordnungen im Internet, In: Internet-Recht und Electronic Commerce Law, Bern 2003, 249 ss. Contra Laurent Moreillon/Aude Parein-Reymond, Code de procedure pénale, Bâle 2013, 752 N 9; Heimgartner, Kommentar zur StPO, N 1a. **27)** The Cantonal Court of Valais on 18 June 2014, c. 4d ("Le blocage provisoire, puis le cas échéant définitif, de l'accès à un blog contenant des propos diffamatoires ne diffère pas fondamentalement du séquestre, puis le cas échéant de la confiscation et de la destruction d'un stock d'imprimés comprenant des propos diffamatoires. On ne voit donc pas ce qui justifierait de traiter la première hypothèse autrement que la seconde, dans laquelle un séquestre en vue de confiscation est indéniablement possible"). This was a revision of the jurisprudence: Cantonal Court of 2 April 2003, JdT 2003 III p. 123, rejecting a blocking injunction because there was no object subject to seizure, then modifying this approach following the judgment of the Federal Criminal Tribunal of 13 February 2005, BV 2004.26, admitting the blocking of websites containing illegal advertisement and medical goods based on the argument that it is proportional to block access rather than seize the servers since "he who can do more can do less"; Cantonal Court of 3 April 2008 ("Bloquer définitivement l'accès à des sites donnés par les moyens techniques appropriés est possible, comme les recourantes l'admettent, et équivaut, dans ses effets, à une destruction au sens de l'art. 69 al. 2 CP. Certes, une telle opinion s'écarte de celle exprimée par l'autorité de céans dans son arrêt du 2 avril 2003. L'arrêt du Tribunal pénal fédéral du 16 février 2005 [...] permet toutefois un tel revirement"). **28)** Swiss Supreme Court, 19 March 2015, 1B_294/2014, c. 4 ("kann offen bleiben, ob die betroffenen Internet- Domains unter die einziehbaren gefährlichen Gegenstände bzw. deliktischen Instrumente subsumiert werden könnten. Die angefochtene Sperrung von Webseiten tangiert das verfassungsmässige Recht des Beschwerdeführers auf Meinungsäusserungs- und Informationsfreiheit. Jede Person hat insbesondere das Recht, ihre Meinung ungehindert zu äussern und zu verbreiten [Art. 16 Abs. 2 BV]"); Cottier, 685. See Guyot/Métille, Le Tribunal fédéral le séquestre pénal d'un domaine ou d'un site web, medialex 2015, 69, which consider that, refusing the analogy (between the blocking as the cessation of illicit behaviour and the destruction as defined by art. 69 al. 2 CP), the Swiss Supreme Court put an end to cantonal judgments which considered that websites made possible the infringiment and, as a consequence, they could be subject to seizure/forfeiture. **29)** Guyot Nicolas/Métille Sylvain (n. 28), 69. **30)** Guyot/Métille (n. 28), 69. **31)** The Swiss Supreme Court accepted to apply CPP 265 to digital data in a decision about the validity of a Vaud Prosecutor's Order against Google respectively Facebook requiring to produce user account data (the user's identity, the IP address used to create the account, the logs over a certain period of time, and the private content of the account) that would have shared some copyrighted works respectively committed insults and calumnies against a Belgian journalist, Swiss Supreme Court, 16 November 2016, 1B_142/2016, c. 3.1 ("Compte tenu de cette lacune, le Procureur pouvait se fonder directement sur la disposition générale de l'art. 265 CPP pour édicter un ordre de production"). However, the Swiss Supreme Court refused to apply CPP 265 in the case at hand, as there was no evidence that the Swiss entity had direct access to data ("Il n'est pas démontré que la société suisse ait un accès direct ou une quelconque maîtrise sur les données relatives à ce service de messagerie") (c. 3.6). It is interesting to note here that, paradoxically, in a decision made one month later, the Swiss Supreme Court considered that the obligation to deposit (CPP 269 ss) was applicable to Gmail's services but refused to apply it for procedural reasons (the measure had not been validated by by the Court) (CPP 273 al. 2) (Swiss Supreme Court, 16 December 2016, 6B_656/2015, c. 1.4.3). **32)** In the "Blogger" decision (n. 28), the Swiss Supreme Court's stance on this issue is ambiguous and the case has been referred to the preceding instance to develop other substantive and procedural issues (suspicions and proportionality). **33)** N. 27 and 28. For general criticisms about the tendency of the courts to apply property law to digital goods, see Benhamou Yaniv, Bien et immatériel: rapport suisse, in: L'immatériel Bien et immatériel: Journées internationales de l'Association Henri Capitant 2014. Bruxelles 2015. 307–330. **34)** Unlike CP 69, they do not require a danger to public safety. ATF 132 IV 55, c. 1a; FF 1985 1061. **35)** Here, the notion of objects or representations is to be understood broadly (e.g. CD, DVD, other electronic media) but it refers to the media as an object. See TPF SK.2007.4 of 4 June 2007, c. 17.1 ("les sites gérés par A. avaient pour objectif principal, sinon unique, d'apporter un soutien aux activités et à la propagande de réseaux terroristes islamiques, en particulier du réseau Al-Qaïda [...] Aux fins visées par l'art. 69 CP doivent ainsi être confisqués, puis détruits, les instruments informatiques (ordinateurs, disques durs, floppy disk, CD-ROM, modem, imprimantes, etc.) ayant été utilisés par les accusés ou par des tiers pour recevoir, alimenter ou créer des liens avec les sites en question, ainsi que tous les écrits, enregistrements sonores ou vidéos reproduisant en tout ou en partie le contenu des mêmes sites"); Moreillon Laurent et al., Petit Commentaire, 2e éd., Bâle 2017, art. 135 CP N 6; Aebersold Peter, Basler Kommentar Strafrecht II, 3e éd., Bâle 2013, art. 135 N 11. **36)** See infra 4. Even acts of violence and terrorism may not be subjet to coercitive measure but only to co-

operative measures. **37)** Even if criminal courts do not have the same freedom as the civil courts to fill in the gaps, they are nevertheless authorized to interpret a norm extensively and to fill any normative gap per se (lacune proprement) by analogical reasoning: ATF 127 IV 198, c. 3b, JdT 2003 IV IV 112; Moreillon et al. (n. 35), art. 1 N 30. **38)** ATF 140 IV 181, c. 2.4, JdT 2015 IV 167, c. 2.6: after the recipient consulted his or her account, before the e-mail cannot be sequestered but only placed under surveillance. **39)** The notion of morality and public order is indeed a broad evolutive notion covering in particular the propagation of negationist statements, ATF 127 IV 203; Hirsig-Vouilloz Madeleine, Commentaire romand du Code pénal I, Bâle 2009, Art. 69 N 27. **40)** "An entity responsible for the central organization, administration, managment of a top-level domain, and the assignment and revocation of user rights on domain names subordinate to it" (Annex ODI). The OFCOM is the register for the ".swiss " TLD and has delegated this task to the Switch Foundation for the ".ch". **41)** Supra n.10. **42)** Cottier, 686, points out that this approach has proven to be effective in certaina areas, e.g. in the fight against child pornography. **43)** Report (n. 2), 31: An action against a participant who cannot reasonably avoid or stop the infringement is therefore doomed to failure. **44)** Report (n. 2), 31, comparing a typical printing house and a hoster by quoting the ATF 126 III 161 (une "imprimerie typique doit toutefois être considérée comme sensiblement plus proche des contenus qu'un fournisseur d'hébergement typique dont les services sont largement automatisés"). **45)** Supra n. 27. **46)** See ECJ C-70/10 of 24 November 2011 (Scarlet c. SABAM), appreciating various fundamental rights, in particular the protection of intellectual property (art. 17.2 Charter of Fundamental Rights), freedom of trade of ISPs (art. 16 Charter of Fundamental Rights, freedom of expression for Internet users and platform operators (art. 11 Charter), protection of privacy and personal data (art. 7-8 Charter of Fundamental Rights). Other fundamental rights have been invoked sometimes (e.g. right to secrecy of telecommunications and data protection) but have not prevented from blocking orders. The secrecy of telecommunications only protects the content of the communication that is not affected by the blocking measure, and not the public information. The data processing is authorized by contract between the user and the ISP. For a more detailed analysis, see Oliver Jo/Blobel Elena, Website blocking injunctions – a decade of development, Schulthess 2017, 27. **47)** See ECHR, judgment of 19 February 2013, Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden (40397/12). **48)** ECJ, judgment of 27 March 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Ors (C-314/12). For national judgments, see references cited by Oliver/Blobel (n. 46), n. 117. **49)** E.g. German Supreme Federal High Court (BGH), judgment of 26 November 2015, Universal Music GmbH et al. v. Telefonica Germany GmbH & Co. OHG (I ZR 174/14), indicating that the blocking measure may not be allowed only with regard to websites offering only illicit content. In some cases, it must be possible even if it leads to suspension of legal content. **50)** ECJ, judgment of 27 March 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Ors (C-314/12), c. 56: "the measures adopted by access providers must be strictly targeted in that they must be used to put an end to the infringement by third parties of copyright or a neighboring right, without affecting the users of the Internet using the services of that provider in order to legitimately access information". The measure ordered for the technique concerned varies from one jurisdiction to another: in Belgium and France the courts generally leave the technical question to the ISP's discretion, while in Denmark and Finland the courts order Exact method of blocking, see Oliver/Blobel (n. 46), 25. **51)** ECHR, judgment of 19 February 2013, Fredrik Neij and Peter Sunde Kolmisoppi (The Pirate Bay) v. Sweden (40397/12). **52)** See UPC Telekabel cited on n. 48, indicating tat the measure should be "strictly targeted". See also ECHR judgment of 18 December 2012, Ahmet Yildirim: the blocking order must be "foreseeable in its application if it is formulated with sufficient precision to enable individuals (...) to regulate their conduct"; See also ECHR judgment of 14 September 2010, Sanoma: "must indicate with sufficient clarity the scope of any such discretion conferred on the competent authorities and the manner of its exercise" (§ 82). **53)** Explanatory Report n. 16, 70–72: "are targeted websites that mainly host pirate offers (pirate sites). It does not cover the offers of works and other isolated objects rendered illegaly accessible on sites offering mainly licit content [...] So are targeted websites that mainly host pirate offers. If a web page makes illegaly accessible only a few works and other protected objects among many licit contents, its blocking would not be proportionate". **54)** Judgment of the Supreme Court of the United States of America of 27 June 2005, 545 U.S. (2005). For an analysis of the judgment, see Urs Portmann/Peter Ling, Le partage de fichier en ligne après l'arrêt Groksoter et dans le projet de révision de la LDA, CEDIDAC 2005. **55)** Art. 27 2.3 Canadian Copyright Act. **56)** ECHR, Neij and Sunde Kolmisoppi v. Sweden, 19 February 2013. **57)** ECHR, Delfi AS c. Estonie, 16 June 2015 (n° 64569/09). **58)** PLDA goes in this direction by recalling that "The measure adopted must also be proportionate on the technical or operational level for the telecommunication service provider" and provides that the ISP may object as set out in art. 66 e, al. 2, let. b. **59)** Report (n.2), p. 47 **60)** Explanatory Report (n. 16), 72. **61)** Equey, 331. **62)** Equey, 330, explaining that the ISP can control these costs using a software allowing to respond to a DNS request, either directly (because it knows the URL) or indirectly (by querying the registry concerned). **63)** See the "Allostreaming" judgment of the Court of Cassation, judgment No. 909 of 6 July 2017 between the Union des producteurs de cinéma à SFR, Orange, Free, Bouygues télécom, et autres. See Oliver/Blobel (n. 48), 19 and the numerous references cited, in particular the Cartier judgment in which the Cour of Appeal gave various reasons justifying that the operator bears the costs. See also Federal Court of Austrlia, judgment of 15 December 2016, Roadshow Films Pty Ltd v. Telstra Corporation Ltd (FCA 1503), where the Court ordered the applicant to pay AUD 50 for each domain name blocked from each ISP but refused to make it bear the general costs because they are part of the "general costs for conducting such activity". **64)** Concerning the reimbursement of such costs in general, see Jeanneret Yvan/Kuhn André, Précis de procédure pénale, Berne 2013, N 5079. **65)** See Equey, 331, indicating that systems are often automated, already in place to block other content (e.g. in the fight against pornography and terrorism) and allow blocking other IP addresses/URLs at lower cost (e.g. via the services "Whitebox" or "Netclean" allowing filtering of the lists of suspicious IP addresses). See Oliver/Blobel (n. 48), 19, mentioning an English ruling in which the marginal cost was seat at £100 per domain name (after an initial set-up cost of £5000) (Court of Appeal, judgment of 6 July 2016, Cartier International AG and Ors v. British Sky Broadcasting Ltd and Ors ([2016] EWCA Civ 658), para. 19). **66)** BGH, judgment of 26 November 2015, (1 ZR 174/14); BGH, judgment of 26 November 2015, (I ZR 3/14). **67)** Explanatory Report (n. 16), 35: the hosting provider intervene (le concours des hébergeurs) in the first place (because they are closer to the content) and ISPs only intervene through access barriers "whether fighting directly against business models based on copyright infringements proves impossible because the operator manages to remain unaffected by a judicious choice of location or by using a jamming technique". **68)** In Swiss law it will be recalled that, case law allows the claimant to act against whom he wishes, supra n. 18. This seems justified as the legal provisions do not provide for such subsidiairity. In European law, art. 8(3) InfoSoc provides blocking measure without requiring subsidiairity and considering it 59 stipulates that blocking must be possible without prejudice to other sanctions. See contribution by Oliver/Blobel (n. 48), 8. **69)** Concerning the right to deindexation under Swiss law, see Meier Philippe, Le droit à l'oubli: la perspective de droit suisse, Lausanne 2015, 23 ss. **70)** See "Allostreaming" judgment of 15 March 2016 of the Paris Court of Appeal, preceding the judgment of the Court of Cassation cited at n. 63. It confirmed both the blocking measures with regard to ISPs and the injunctions of deindaxion concerningt the search engines (e.g. Google, Yahoo). **71)** See Oliver/Blobel (n. 48), 23 giving the example of The Pirate Bay, which has used various domain names since 2012, including .org (which has been no longer used after an American proceeding), .se (which has been no longer used after the seizure of the domain name in Sweden), .gs, .la, .mn, .am et .gd **72)** ECJ, judgment of 27 March 2014, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH and Ors (C-314/12), c. 58 ss.; ECJ, judgment of 24 November 2011, Scarlet Extended SA v. Société Belge Des Auteurs, Compositeurs et Éditeurs SCRL (SABAM) (C-70/10), c. 43; Submissions of the Advocate-General Szpunar of 8 February 2017, Stichting Brein v. Ziggo BV and Ors (C-610/15), c. 78. **73)** Brett Danaher/Michael D. Smith/Rahul Telang, Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior, Pittspurg 2016; Site Blocking Efficacy Study United Kingdom, Incopro, 2014. **74)** Equey, 332. **75)** See Oliver/Blobel (n. 48), 23. **76)** High Court of Justice, Chancery Division, judgment of 13 March 2017, The Football Association Premier League Limited v. British Telecommunications Plc and Ors ([2017] EWHC 480 [Ch]). **77)** Bohnet, N 86. **78)** Hofmann, 208: with the direct execution, the measures requested shall be taken by the Court seised to determine the merits of the dispute: in its formal judgment, the Court may, at the request of one of the parties, order the enforcement of its decision or set the conditions of it (art. 236 al. 3 CPC; art. 337 al. 1 CPC). **79)** Hofmann, 209: after the application for enforcement has been filed, the enforcement Court shall of its own motion examine the enforceability of the decision (art. 341 al. 2 CPC) and set a time limit for the responding party to rule on the application (art. 339 al. 2 CPC) (which may, in particular, argue that the condition has not been fulfilled or the consideration has not been made) before deciding on an (indirect) implementing measure among those provided by the Article 343 CPC. **80)** Report (n. 2), 31: An action against a participant who cannot reasonably avoid or stop the infringement is therefore doomed to failure. **81)** Report (n. 2), 31, comparing a typical printing house and a hosting company by quoting the ATF 126 III 161 (une "imprimerie typique doit toutefois être considérée comme sensiblement plus proche des contenus qu'un fournisseur d'hébergement typique dont les services sont largement automatisés"). **82)** Explanatory Report (n. 16), 73.