Journal of Contemporary European Research

Volume 9, Issue 1 (2013)

Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content

Katalin Parti *National Institute of Criminology*

Luisa Marin *University of Twente*

Citation

Parti, K. and Marin, L. (2013). 'Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content', *Journal of Contemporary European Research*. 9 (1), pp. 138-159.

First published at: www.jcer.net

Abstract

Removing illegal or harmful material from the internet has been pursued for more than two decades. The advent of Web 2.0, with the prominent increase and diffusion of user-generated content, amplifies the necessity for technical and legal frameworks enabling the removal of illegal material from the network. This study deals with different levels and methods of Internet 'cleansing' measures, comparing government regulated and Internet service provider based removals of illegal Internet content. The paper aims at putting the regulatory option of internet blocking measures into the broader perspective of the legal framework regulating the (exemption from) liability of Intermediary Service Providers (ISPs) for user-generated contents. In addition, the paper suggests proposals on which regulatory options can better ensure the respect of freedoms and the protection of rights. The paper introduces several significant cases of blocking online copyright infringing materials. Copyright related blocking techniques have been devised for business reasons – by copyright holders' associations. It must be recalled, however, that these blocking actions cannot be enforced without the states' intervention. These business-level actions become isolated if they are not supported by both the European Union and its Member States. Conversely, state-centred initiatives cannot work out without the private sector's cooperation. Internet service providers play a crucial role in this cooperative framework because of their task of providing access to the Internet and hosting web contents.

Keywords

Soft-Law regulation; Self-Regulation; Hard-Law Regulation; Internet Blocking; Notice and Take-down procedures; Intermediary Service Provider, Liability; E-Commerce Directive

---

In the past 20 years there have been many attempts to remove illegal or harmful online content. The first solutions were devised to block unsolicited electronic advertisements, so called *spam*, so that junk mail does not slow down the speed of internet connections. These solutions were applied by users individually, and also often by ISPs for the protection of their users. The need to block unwanted content, however, gradually appeared on higher levels with time.

There are several regulatory options to remove illegal internet content.[1] Solutions for blocking illegal Internet content usually require the substantial involvement of base level actors, such as private users and ISPs. This refers to decentralised, partially self-regulated, or bottom-up measures applied by private parties such as users and ISPs. A decentralized enforcement measure includes *primary, user-level protection* with firewalls, and filter software, whereas institutional filter measures protect users more at the community-level, for example when a school, library or employer filters contents in the interests of their users (schoolchildren, visitors to the library, employees). Another *regulatory option* is characterised by the ISP's intervention, installing filter software in their systems that stop unsolicited advertisements and junk mail to get through to the users. The introduction of *shared filter systems* designed by several service providers jointly is usually applied on the basis of codes of conduct. Such filters also function as quality assurance, and are installed to guarantee service quality on the one hand, and to provide equally high quality service to all users on the other, blocking unsolicited mail and ads. In this sense, private regulatory measures are applied ex post, when infringement of copyright or individuals' rights are detected. Another instrument is the

[1] Illegal internet content is a category which is not yet defined at the European level, as it relates to the national legislation of the Member States. Recently, the European Data Protection Supervisor (EDSP) has expressed the necessity for "a more pan-European harmonised definition of the notion of 'illegal content' for which the notice-and-action procedures would be applicable". See: 'EDPS formal comments on DG MARKT's public consultation on procedures for notifying and acting on illegal content hosted by online intermediaries', p. 1.

N&TD procedure, foreseen by Article 14 of the e-Commerce Directive.[2] This requires that, whenever the ISP has knowledge of illegal activity, it should act expeditiously to remove or disable access to the information. This means that the action is taken ex post, only when there is a notice of an illegal material by a user or other actor. According to the directive, the procedure can be more or less forged by Member States' legislations, and thus involves court or administrative authority. Actually Member States are entitled to establish procedures governing the removal or disabling access of information. This is also an element of decentralization. The practical enforcement of this process welcomes the contribution of private actors involved, through codes of conduct. In this respect, one should observe that N&TD procedure could be framed as decentralised, multi-actor driven and ex post.

By contrast, we have another regulatory option for dealing with illegal internet content, i.e. blocking measures. As such, this regulatory option implies a choice for centralised and ex ante process of indicating the illegal internet content, and the ISPs are required to enforce it. This option is acknowledged as potentially the most invasive regulatory option, so its impact on individual freedoms has to be considered. Within the framework of blocking measures, state enforcement agencies usually require ISPs to block contents that are illegal or constitute serious crimes. Obliging the ISPs to monitor and filter users' online activities and remove all 'illegal content' found in their network is a top-down initiative introduced by the governments as ex ante solutions, and have to be followed strictly by the private sector. This solution provides a stroke-of-the-pen removal of illegal contents in a standardised process. However, such centralised, ex ante, and top-down measures can breach ISPs' rights to freely conduct business, as well as individuals' rights to privacy, free speech and the protection of personal data.

On the other hand, decentralised regulatory models have also their weak points as such measures can be institutionalised in different ways, providing different rules for the removing process thereby undermining the success of the removal. Decentralised regulation is not unified, as we cannot be sure whether all public institutions indeed install filter software. Moreover, certain methods are not capable of blocking all illegal content. A typical example of this is keyword filtering applied by users, where there is a danger of over- or under filtering, and it is often determined by the level of experience of a given user and his skills. A further problem may arise when the software only filters content it was ordered to filter by the user, but other illegal websites are allowed through, or when a child easily bypass the filter settings of the parent. In the following section, we will discuss some of the controversial aspects of central level internet-blocking initiatives.

BLOCKING MEASURES AND THE EUROPEAN FRAMEWORK REGULATING ISPs' LIABILITY

As internet access became more publicly available, content-related crimes ensued. The European Union recognised the threats posed by the dissemination of harmful online content relatively early, and therefore started the work on establishing the foundations of concerted protective measures in the late 1990s, as it is also clear from the arsenal of European and international regulations related to the sexual exploitation of children,[3]

[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), [2000] OJ L178/1.

[3] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25.10.2007 (CETS No.: 201); Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography Official Journal L 013, 20/01/2004 P. 0044 – 0048; and Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA Brussels, 29.3.2010 COM(2010)94 final.

cybercrime[4] the global fight against terrorism,[5] attacks against information systems,[6] and organised crime,[7] just to mention the most important ones. Though the above listed regulatory pieces do not necessarily mention removing, or blocking, access to illegal internet content, the aim of the Member States of jointly stepping up against the illegal contents suggests the need of developing centrally coordinated protective measures in the realm of the internet thereby protecting its citizens. However, in so doing, precautions must be taken so that the state does not prejudice basic citizens' rights (freedom of speech, expression and information) while protecting the citizens, ensuring national security and enforcing the law (Magaziner 2000).

The outer boundary: the European Convention for Human Rights

While the States' intentions to regulate internet can be justified with the protection of legitimate purposes, such as crime fighting and rights' protection, the same attempts can also disguise surveillance purposes, which eventually could undermine the overall freedom *of* internet and freedom online. That is why it is important in the governance of the internet that every public power's intervention is justified by an overriding public interest, secured by the compliance with the legality principle, and bound by a full respect of the principle of proportionality. This outer boundary to the freedom of internet has been put also by a judgment of the European Court for Human Rights, in the case of K.U. v. Finland.[8] More precisely, the merit of this judgment is to provide an outer boundary to the freedom of confidentiality of the internet service provider, which cannot lead to the point that unlawful activities cannot be taken to justice. In the specific case, the applicant was 12 years old when an unknown person had placed without the applicant's knowledge an advertisement on a dating Internet site in his name. The advertisement contained some of the applicant's personal information (name, phone number, link to a personal page with photo and other details) and included a sexual connotation. The applicant became aware of this as he was exposed to grooming behaviour from persons on the Internet.

Under the Finnish regulation in place at that time, the internet service provider refused to reveal the identity of the IP address-holder in question under the law of confidentiality in telecommunications. The Helsinki district court refused to oblige the service provider to disclose the telecommunications identification data in breach of professional secrecy, lacking an explicit legal provision authorising it. More precisely, 'malicious misrepresentation', was not an offence authorising police to obtain telecommunications identification data under the legal provisions of the time. This position was upheld by supreme domestic courts. The final result was that the applicant never got access to the identity of the person in question, and the managing director of the Internet service could not be prosecuted because the alleged offence had become time-barred.

The Strasbourg Court found that this case violated the right to private life, as defined in Article 8 of the European Convention of Human Rights, 'a concept which covers the physical and moral integrity of the person'.[9] In the reasoning of the Court the right protected at Article 8 does not lead merely to a negative obligation from the state, but entails also a positive obligation that 'might involve the adoption of measure designed to secure respect for private life even in the sphere of the relations of individuals among

[4] Convention on Cybercrime of the Council of Europe of 23.11.2011 (CETS No.: 185).
[5] EU Council Framework Decision 2002/475/JHA of 13.6.2002 on combating terrorism (O J L 164/3 of 22.6.2002) as amended by Council Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008); Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (CETS No.: 196).
[6] EU Council Framework Decision 2005/222/JHA of 24.2.2005 on attacks against information systems (OJ L 69/67 of 16.3.2005).
[7] United Nations Convention Against Transnational Organized Crime of 8.1.2001 (A/Res/55/25).
[8] Judgment of 2 December 2008, K.U. v Finland, application no. 2872/02.
[9] See Court's judgment, para. 41.

themselves'.[10] States do enjoy a margin of appreciation in fulfilling the obligation arising from the Convention, a margin which is nevertheless bound by limits. The Court, while acknowledging that 'freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and internet services must have a guarantee that their own privacy and freedom of expression will be respected', takes the position that 'such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.'[11]

THE ISP'S LIABILITY FOR USER GENERATED CONTENT

The underlying question is whether the ISP can be held liable for user-generated content, and if so, under which circumstances and conditions. ISPs are service providers offering access, data transmission, storage space, proxy, and/or search services to content providers (users). The liability of ISPs is regulated at EU level by the Directive 2000/31/EC on e-commerce (hereinafter E-Commerce Directive).[12] The E-Commerce Directive aims to harmonise national laws on information society services relating to the internal market and, among others, the liability of such intermediaries in order to contribute to the 'proper functioning of the internal market by ensuring the free movement of information society services between the Member States.'[13]

The Directive grants the service provider exemption from liability for the services of "mere conduit", "caching" or "hosting". The ISP is not responsible for contents uploaded by users, neither for copyright or privacy infringements, nor for damages, as so far certain conditions. The ISP must not have initiated the uploading or transmission itself, and should not have been involved in the selection of receiving parties, or sorted or modified (edited) the contents uploaded by the users. This includes the automatic transmission of data and the transitional or temporary storage of these provided that the service exclusively includes data transmission and storage, and that the service provider did not store the data transmitted this way longer than the minimal length of time needed for transmission.[14]More precisely, and defining "mere conduit", the E-Commerce Directive stipulates that if the service provided by the ISP consists of the 'transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network', the ISP shall be exempted from liability if it: '(a) does not initiate the transmission; (b) does not select the receiver of the transmission; and (c) does not select or modify the information contained in the transmission.'[15]

The legal framework for hosting services has the same *rationale*. Given that "hosting" consists in the storage of information provided by a recipient of the service, the ISP is exempted from liability if it does not have 'actual knowledge of illegal activity or information', or, 'upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information'. There is no general obligation to monitor bearing on the ISP, nor a general obligation of actively seeking facts or circumstances indicating illegal activity. However, Member States may well establish obligations 'promptly to inform the competent public authorities of alleged illegal activities undertaken or information provided by recipients of their service or obligations to

[10] *Ibidem*, para. 43.
[11] *Ibidem*, para. 49.
[12] Directive 2000/31/EC of The European Parliament and of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) Official Journal L 178, 17/7/2000 P. 0001-0016.
[13] Quotes from Art. 1, E-Commerce Directive.
[14] See Preamble (46) and Art. 12-14 of the E-Commerce Directive.
[15] Art. 12, E-Commerce Directive.

communicate to the competent authorities, at their request, information enabling the identification of recipients of their service with whom they have storage agreements.'[16]

Furthermore, once an illegal activity is ascertained, according to the Member States' legal systems,[17] the ISP has the duty to cooperate with public agencies in the removal of the breach: every provision granting exemption from liability is indeed closed by a corresponding provision enabling domestic courts, or administrative authorities, to require the ISP to terminate or prevent an infringement.[18] As to hosting services, Member States are entitled to 'establish procedures governing the removal or disabling access to information.'[19]

The highly controversial[20] Data Retention Directive[21] (DRD) also regulates ISPs' obligations. It 'aims to harmonise Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime.'[22] The Directive orders Member States to regulate ISPs to catch traffic, location and related data types and keep it for 6 to 24 months. When the ISP gets an order from the local law enforcement agencies, it has to transmit the stored data for investigatory and jurisdictional purposes. One can argue that this is an obligation involving monitoring activity. However, ISPs could monitor their users' activity even without catching and storing their data, and moreover the DRD does not explicitly refer to "monitoring". On the contrary, it highlights that the ISPs only have to 'retain' certain data categories from deletion. Nonetheless, most of the data types addressed by the DRD are so called Charging Data Records (CDRs) which are recorded by the ISPs automatically, for business purposes, in order to charge users for the service. There are significant debates in the Member States criticising the transposing legislations for infringing civil rights on grounds of legality and proportionality, as well as for breaching the traditional data protection principle of purpose limitation. Several Member States' attempts to transpose the directive to national legislation have been subject to constitutional challenges for the very reasons indicated above.[23] The constitutional challenges DRD faced at domestic level have urged the Commission to prepare a recast. However, considering the prejudicial nature of another piece of legislation, the e-Privacy Directive,[24] the recast of the DRD has been put on hold.[25] However, the DRD is not aimed to plant the task of "monitoring" or "investigating" in the hands of the ISP. Consequently, their liability does not embrace a responsibility for user generated content either. The most recent European legislation confirms the limitation of the liability of the provider: directive

[16] Art. 15, E-Commerce Directive: "No general obligation to monitor".
[17] See Art. 12, para. 3; Art. 13, para. 2; Art. 14, para. 3, E-Commerce Directive.
[18] See Art. 12, para. 3; Art. 13, para. 2; Article 14, para. 3, E-Commerce Directive.
[19] Art. 14, para. 3.
[20] According to the European Data Protection Supervisor the DRD is "the most privacy invasive instrument ever adopted by the EU". Source: European Data Protection Supervisor, 'The moment of truth for the Data Retention Directive', 3 December 2010, p.1.
[21] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105/54, 13.4.2006.
[22] Art. 1 para. 1, DRD.
[23] In 2009 Romania, in 2010 Germany, and lately, in 2011 the Czech Republic, Cyprus and Lithuania.
[24] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[25] Source: Statewatch: "EU: Revision of Data Retention Directive put on hold with "no precise timetable" for a new proposal". At http://www.statewatch.org/news/2012/aug/04eu-mand-ret.htm, accessed 11.09.2012.

2009/136/EC[26] reaffirms that the provider cannot be liable for merely transmitting user-generated information ("mere conduit" rule), and confirms that it is not a provider's task to define what is lawful or harmful in respect of content, applications and services. According to the directive, the ISP has still no obligation to monitor contents, and therefore has to remove the content concerned by a notice.

According to the legal pieces referred to above, it is mainly the producer of the content who is responsible for the content published online. So if the publication of the content involves copyright infringement, or does not respect the privacy rights of others, the European regulator has placed the liability only on the content's uploader (Viola de Azevedo Cunha et al. 2012). In a typical case, the producer of the content is the individual user, who as such uploads his family videos to an online video sharing channel, uploads his images to a social network site, publishes his opinion in a blog or forum, or creates online content in another way (e.g. edits websites). The question is when the service provider actually qualifies as a content provider. For example, can and should s/he be held liable as a content provider, albeit not uploading the content itself, it nevertheless has classified it and selected it on the basis of some principles (popularity index, compliance checklist, etc.)? Is the service provider a content provider if it adds new content (hyperlinks, advertisements, etc.) to the original one uploaded by the user? Advertisements may be further divided into ones of a content related, or not related, to the user-content (published independent of the latter on the same site), and into profit-oriented and non-profit advertisements.

If the ISP only ensures the technical platform and conditions for uploading contents and an access to the internet, the question arises in which cases it is actually responsible for the contents uploaded by the user. If it was aware of the content being illegal and did not remove it within the required timeframe (which further brings up the question whether it has to wait until the notification and removal request to the user, or has to remove the illegal content without such); or if it was not aware of the content being illegal, but it edited, labelled and forwarded it; and if it was not aware of the content being illegal, and it only provided the technical platform for its publication. In the latter two cases the question also arises whether the service provider has a surveillance obligation; that is whether he has to monitor the legal compliance of content published on his platform.

Some clarification comes from the recent case law of the European Court of Justice (ECJ), in particular the judgments *Google v. Louis Vuitton*,[27] and the *L'Oréal v. eBay* case.[28] While in the first case, the Court has recalled that the neutrality principle is the basis for the exemption from liability, in the second case the Court took the approach that if an operator of a marketplace plays an active role, it can therefore not be exempted from liability granted by the Article 14 of the E-Commerce Directive, referring to "hosting" services.[29] The Court further stated that 'Where, by contrast, the operator has provided assistance which entails, in particular, optimising the presentation of the offers for sale in question or promoting those offers, it must be considered not to have taken a neutral position between the customer-seller concerned and potential buyers but

[26] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. Official journal L 337 18.12.2009 P. 0011-0036.

[27] European Court of Justice, Joined Cases C-236/08 to C-238/08, Google France, Google, Inc. v Louis Vuitton Malletier (C-236/08), Viaticum SA, Luteciel SARL (C-237/08), Centre national de recherche en relations humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08), Judgment of the Court (Grand Chamber) of 23 March 2010, [ECR 2010-2417].

[28] European Court of Justice, Case C-324/09, *L'Oréal v eBay*, Judgment of 12 July 2011, OJ C 269, 10.09.2011, p. 3.

[29] *L'Oréal v. eBay*, para. 123.

to have played an active role of such a kind as to give it knowledge of, or control over, the data relating to those offers for sale. It cannot then rely, in the case of those data, on the exemption from liability referred to in Article 14(1) of Directive 2000/31.'[30]

Considering that recent internet platforms run by global commercial companies have shaped a new generation of internet sites labelled under Web 2.0, it is all the more relevant to analyse whether the legal framework in place can still offer solutions that can be working also for new situations. It is not a case that Advocate General Jääskinen, in its Opinion on the *L'Oréal* case, has criticized the neutrality principle as the basis for the exemption from liability, principle upheld by the Court in its earlier case *Google v. Louis Vuitton*. The Advocate General has suggested avoiding to sketch out parameters of a business model that would fit to the hosting exemption, proposing to focus instead on the type of activity, and state that 'while certain activities [...] are exempted from liability, as deemed necessary to attain the objectives of the directive, all others [...] remain in the 'normal' liability regimes of the Member States'.[31] Then the question remains: can the plethora of internet pages of the Web 2.0 still benefit from the neutrality principle, which entails that the activity of the ISP is 'of a mere technical, automatic and passive nature', and that the service provider 'has neither knowledge of, nor control over the information which is transmitted or stored'?[32]

REGULATORY OPTIONS FOR BLOCKING ILLEGAL CONTENT IN PRACTICE: THE GERMAN AND THE HUNGARIAN CASE

In the past few years, there have been several solutions for centrally filtering illegal content spread over the internet. In addition to the instruments of blocking not being too effective, these also demand a significant effort, and involve the infringement of citizens' rights.[33] The government-level control of the internet is most often implemented as part of the efforts to fight online child abuse, or other harmful actions that are considered to be dangerous to individuals and the public. However, the lesser the damage caused by encountering the given contents on the user's website is, and the longer the causal chain between the damage suffered and encountering the content; the less justification is there for applying such harsh measures as blocking content. In this section, we introduce a few solutions that governments apply in order to comply with their obligations regarding the blocking of illegal content.

Germany is the economic engine member of the European Union, which is reflected by the fact that it is one of the countries of the world having the highest level of internet access and penetration.[34] On the account of its historical experiences, considerable efforts have been taken to balance security measures and citizens' freedoms and rights. Consequently, it is one of those European countries where civil rights' defenders speak out loudest against centrally generated internet blocking measures. Based on this the German case is discussed in much details concerning regulatory options.

German law has implemented the "mere conduit" rule of the E-Commerce Directive in Section 10 of the multimedia act (*Telemediengeset*z: TMG). Under the said section, the ISP cannot be held liable for user-generated content, except if it fails to identify contents

[30] European Court of Justice. Case C-324/09. Judgment of 12 July 2011, para. 116.
[31] Advocate General Jääskinen, Opinion on the case *L'Oreal v. Google*, para. 149.
[32] *Google v. Louis Vuitton*, cit., para. 113.
[33] For a recent and holistic approach see: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. United Nations Human Rights Council. Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf; [11 October 2011]
[34] Germany ranges the sixth country in the world, and the first in Europe with the highest number of internet users (67,4 millions of users). http://www.internetworldstats.com/stats.htm, accessed 27 September 2012.

as illegal due to negligent ignorance or contingent intent (*dolus eventualis*). Analogous to that – in accordance with the Teleservices Act (*Teledienstgesetz*: TDG) and the contract of the German state with media service providers (*Mediendienstestaatsvertrag*: MDStV) – the access-provider cannot be held liable for damage caused by users to third parties on websites offering auction services if a provision to that effect is contained in the general terms and conditions. However, there may still be accessory liability of the service provider in some cases. In that sense, the direct offender (the user) is not solely responsible for the damage he causes to third parties, and the service provider, who knowingly or casually contributes to the infringement of the rights of the third parties, has also liability: provided that the service provider had no obligation to observe in the first place. In line with a decision of the Federal Court of Justice, as soon as the ISP gains knowledge of the infringement of a third party's rights, he has to take immediate precautions to avoid a repeated offence (by removing the content, blocking the infringing user, or suspending the user's rights).

In Germany, a bill[35] proposing the blocking[36] by ISPs of child abuse depictions spread over communication networks was published on May 5, 2009. According to the bill, the Federal Criminal Police Office of Germany (*Bundeskriminalamt*: BKA) has to maintain a list of FQDNs,[37] IP-addresses and URLs to multimedia materials, which under the German criminal code contain child pornography, or which refer or contain links to such content. The BKA issues an updated blocking list every working day for bigger ISPs to whom the legislation applies. ISPs serving at least 10,000 users in their normal course of business have to take all 'appropriate and due technical steps to block the access to multimedia content featured on the list' within six hours at the latest. The blocking must be realised at least on "domain-level". The ISP has to inform the user who published the illegal content of the reasons for the blocking and the contacts of the BKA by way of a "stop notice", in case the originator of the content should object to the blocking. Service providers carrying out blocking measures are entitled to collect and use personal data, to the extent necessary for the blocking, and are obliged to hand over these data to the investigative authority for the purpose of criminal proceedings. The bill was adopted at the meeting of the German parliament on 18 June 2009. The legal instrument entered into force in February 2010, but could not be enforced, and lately the disputed law has been dropped.[38] The act was attacked on the grounds of not being satisfyingly efficient, while it intervenes disproportionately in the practice of fundamental citizens' rights, and does not spare the rights of the internet service providers either.

Blocking may often have harmful side-effects; simple blocking methods (such as the German solution, that is the DNS-level manipulation of domains) are often not too effective, as illegal and legal contents belonging to the same domain name cannot be clearly separated which can result in either over- and under-filtering. Contents are often over-filtered; legal contents, or links to legal websites, are often blocked from access curbing the freedom of information. However, as a result of the same method, under-filtering can take place as well, thus illegal contents can remain available. The German solution has one rather special aspect, namely that it only applies to contents available

[35] Entwurf eines Gesetzes zur Bekampfung der Kinderpornographie in Kommunikationsnetzen. Drucksache 16/12850, 05.05.2009, and Gesetzesbeschluss des deutschen Bundestages. Drucksache 604/09, 19.06.09 Available: http://www.bundesrat.de/cln_090/SharedDocs/Drucksachen/2009/0601-700/604-09,templateId=raw,property=publicationFile.pdf/604-09.pdf, accessed 12 April 2010.

[36] Even though semantically speaking filtering and blocking do differ – in that filtering involves monitoring, while blocking the prevention of the dissemination of already identified content –, we wish to use these expressions synonymously in this study.

[37] *Full Qualified Domain Name*, which exactly defines the location of the domain in the domain hierarchy.

[38] In February 2011 the German Working Group against Internet Blocking and Censorship (AK Zensur) lodged their complaint against the German law on Internet blocking to Germany's Constitutional Court. In April 2011, Germany's governing Conservative and Liberal parties agreed in a coalition committee meeting that the disputed law on Internet blocking of child abuse material will be dropped. Source: German Internet blocking law to be withdrawn. Available at: http://www.edri.org/edrigram/number9.7/germany-internet-blocking-law, accessed 1 November 2011].

through bigger German access providers, so those who access the Internet through smaller, or foreign service, providers, can still access the illegal content.[39]This situation shows how the ubiquity of internet hardly can be controlled and counteracted through a State's unilateral measures, which are mainly limited to enforcement within the territory of the State. The efficiency of blocking is not proportionate to the degree of intervention in constitutional rights and fundamental freedoms, as blocking measures affect the freedom of information and expression, while they do not ensure necessary protection to victims and users.

It is often mentioned that one of the positive results deriving from the introduction of domain-based blocking in Germany is that the online surfing of users also can be tracked. This offers the opportunity for launching criminal proceedings against the "consumers" of child pornography. The most important principle of the concept is that blocked domains point to child pornography contents; therefore criminal proceedings can automatically be launched against those who try to bypass the block, e.g. by switching to other service providers' network. Bypassing the block would namely be evidence for the intentional nature of the preparation for acquisition of the illegal material (offending behaviour). (Sieber 2009: 657) A further concern regarding the German legislation is that the blocking list may be compiled and updated without a judge's approval, as there is no independent body assigned to supervise the decisions of the investigative authority. The critics claims that the black list (according to which the ISPs would be obliged to block illegal contents) cannot be compiled by one single authority; just the updating process would be an excessive burden for the BKA's personnel. In addition, an independent control function as a guarantee of free speech should be embedded into the process by the court, in accordance with a general normative perspective.

The liabilities of the ISPs legally required to block was not defined in the German act in depth. It was also unclear which was the obligation of the service provider as to blocking, considering that the legislation only prescribes the "minimum" level of blocking of domains for service providers. Furthermore, whether the service provider has other obligations in relation to blocking was not defined by the law. (Sieber 2009) According to this piece of legislation that finally did not enter into effect, the German multimedia act (TMG) stipulated that if the internet service provider had implemented the blocking as required, he was acquitted of any responsibility in respect of all illegal content allowed through (safe harbour clause). However, the act did not stipulate what steps the service provider should take after implementing blocking measures according to requirements, but without positive results. It was not clear whether the service provider is acquitted from his obligations if he introduces further blocking measures that continue to be unsuccessful. Moreover was unclear whether internet service providers might have claims to damages vis-à-vis the State in relation to the collateral blocking of legal content.

TMG stipulated that access providers have to record the data of users publishing illegal content on domains featured on the blacklist, and surrender those to the investigating authority for law enforcement purposes. This way, however, not only the data of those publishing the contents, but also the IP-addresses of those downloading the same contents could be established by the investigative authority. This meant that the service provider interfered with the rights of the users to freely dispose their information, and that downloading blacklisted contents might be compromising to the users and misleading for the investigative authority. There might have been investigations which have been launched in cases where the *legal* website, which the user was actually looking for, contained an illegal link or featured on the blacklist.

The above described domain-based internet-blocking technology, relying on blacklists and the concept built on it, are not proportionate to the envisaged goals. Due to over-filtering, it intervenes more drastically in the basic freedoms of citizens than the severity

[39] On reliability of blocking measures see http://www.opendns.com, accessed 1 November 2011.

of the damage caused by the online behaviour.[40] Child pornography, and the related phenomenon of paedophilia, is among the most serious crimes, which also the ECtHR requires States to be especially vigilant on. However, it is important to understand that it is *not* the freedom of expression of criminal offenders and the freedom of getting (illegal) information that is compromised by blocking illegal content. But central (government-level) blocking measures are inappropriate, because they usually apply domain-based blocking, as described in the German case above, which blocks not only illegal internet contents, but impairs such functions as mailing and other online services (e.g. IGroups services) not illegal as an application in itself. Moreover, with the continuous extension of blocking lists, more and more legal content and internet-functions may be lost.

The system of links and hyperlinks, and the liabilities for contents that the links and hyperlinks point to are not regulated by either the Council of Europe, or the European Union, so it comes down to the national legislation of the Member States. In Germany, court practice (in this case a court rule of the Berlin municipal court in 1997) equates liability for links and hyperlinks with the liability for the creation of websites (and content provision). The rule of the Berlin court stipulated that a hyperlink pointing to a website containing illegal content has the same promoting and encouraging effect to the crime, as the website itself, for which reason it is as much an object of crime as the website's content.[41] This in turn constitutes a basis for the liability for contents made available in the indirect system of links.[42] The liability of search engine operators in Germany is not clearly regulated, as the legal regulations have no relevant provisions, and the case law on the matter is not consistent. In a case initiated on the grounds of a lawsuit filed by trademark holders, several lower courts has established that operators of search engines are not accountable as accessories for the trademark infringements committed by their users, not even if the users carried out their actions by opening (clicking on) ad-words and sponsored links they themselves placed there. Using the very opposite logic, however, courts established the accessory liability of search-engine service providers for the placement of sponsored links pointing to foreign online gambling websites.[43]

Despite the fact that the above described legal regulations on internet blocking have not entered into effect, there is a practice of blocking illegal online content in Germany on a case-by-case basis as it is unconstitutional to propagate any Nazi ideology in Germany. Such was the 2002 order of the district government of Düsseldorf for blocking, which bound the German access providers not to allow Nazi propaganda through websites hosted on US servers.[44] The higher administrative court of Münster acceded to the blocking order, and in their reasons described that the blocking order concerned is necessary to stem the revival of the German extreme right-wing ideology. Such a blocking order, however, has to meet the requirements of proportionality and technical plausibility. The occasional orders for IP-address blocking, domain name server modification and proxy server installation to access providers from courts are good

[40] There is no research available as to what actual damage is caused by encountering depictions of child pornography – neither among adult or child Internet users. It is on the other hand clear that by only applying central filtering, users may not be protected from encountering illegal content. For this reason, every Internet filtering measure should be accompanied by appropriate information (dissemination of knowledge, education, danger-awareness) specialized for specific age groups. For more see: See also: „A Google és a Yahoo is az ausztrál Internetellenőrzési tervek ellen" Sg.hu, Informatikai és Tudományos Hírmagazin February 18, 2010 Available at http://www.sg.hu/cikkek/72596/a_google_es_a_yahoo_is_az_ausztral_internetellenorzesi_tervek_ellen, accesed 18 Ferbuary 2010.

[41] AG Berlin, 260 DS 857/96, 30. Juni 1997: http://www.netlaw.de/urteile/agb_01.htm, accessed on 18 February, 2010.

[42] The responsibility for content made available through other technical solutions – such as by search engines – is not clearly defined.

[43] Study on the liability of Internet Intermediaries. Country Report – Germany. By prof. dr. Gerald Spindler, University of Göttingen, 2007 Available at: http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/germany_12nov2007_en.pdf, accessed 12 October 2011.

[44] Bezierksregierung Düsseldorf, Aktenzeichen 21.50.30, 6 Februar 2002 Available at: www.artikel5.de/rohetexte/sperrverfueg.pdf, accessed 12 October 2011.

examples. Meanwhile, the Bundesgerichtshof ruled out in 2000 a new principle, according to which e.g. the content provider of a website denying the Holocaust uploaded to a server in Australia can be held liable for the crime (denying the Holocaust) in Germany, even if the offender is an Australian citizen. The decision, however, clearly ruled that the ISP hosting the illegal content cannot be held liable.[45]

In several EU Member States, courts have developed a measure called ''notice and stay down'', applied instead of the ''notice and takedown'' measure introduced by the E-Commerce Directive. According to notice and stay down, search engine providers like Google are obliged to introduce a permanent monitoring system which permanently survey and filter out illegally uploaded and circulated internet content – without a notification from the authorities. In July 2012 the Paris Court of Cassation laid down decisions in four different cases annulling the monitoring obligations of the ISPs ordered by lower courts, and reintroducing notice and takedown measure into the practice as it is stated by the E-Commerce Directive. Consequently, ISPs are no longer obliged to identify and remove illegal internet content without order, only when the entitled party warns it to do that. Similarly, a July 2012 court rule of the High Court of Hamburg obliges a file-sharing service provider to monitor the files shared on its network. The decision prescribes RapidShare file-sharing provider to actively monitor the files appearing on its site, and remove illegally uploaded (shared) ones. According to the decision, providing the space for file-sharing is not a passive service, but an active one – as it is "sharing" and not "storing" files. The provider becomes an accomplice of the file-sharer, as he facilitates file-sharing.[46] These decisions are followers of the Court of Justice's statement dating back to late 2011. In November 2011 the European Court of Justice stated, that Member States must not put ISPs under any obligation to endorse illegal police activities and thus providing surveillance of users.[47] The ECJ ruled that national court's order to force ISPs to implement filter systems, installed at ISPs' own expense and used for an unlimited period of time, would breach the ISP's rights to conduct business freely, and would infringe individuals' rights to privacy and personal data protection.

The impact of German law making and court decisions is neither economically, nor politically negligible for other European countries. In this respect, especially transitional countries of Eastern and Central Europe have to be mentioned, whose legal development has historically been influenced by the German law-making traditions for centuries. Hungary is one of these countries. Besides that it is historically linked to Germanic traditions by several strings, the Hungarian development is worth analysis because its development on the field of internet freedom is, paradoxically, diametrical. While Hungary as a member state of the European Union has to comply with EU law, its national case law does not reflect the Union's law. An example of this is the deficit of handling illegal content hosted on servers in foreign countries.[48] Nevertheless a rather radical step was taken by the lawmakers when 'making illegal Internet content unavailable will be introduced as a new sanction into the criminal code in2013. This

[45] Az: 1 StR 184/00 vom 12. Dezember 2000 Available at: www.rechtsanwaltmoebius.de/urteil/bgh_auschwitzluege.pdf, accessed 12 October 2011.
[46] Julien, L.: Allemagne: RapidShare doit surveiller les contenus après notification. Numerama, 17 July 2012. http://www.numerama.com/magazine/23198-allemagne-rapidshare-doit-surveiller-les-contenus-apres-notification.html.
[47] Judgement of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Societé belge des auteurs, compositeurs et édieurs SCRL (SABAM) http://curia.europa.eu/juris/document/document.jsf?docid=115202&doclang=EN&mode=&part=1, accessed 21.09.2012.
[48] For instance, until this day, not an adequate legal answer could be taken against Kurucinfo.hu portal, which is a Hungarian language website inciting to hatred against Hungarian minority groups, hosted by a U.S. based server.

sanction will be imposed against the user who uploads illegal material, obliging the service provider to remove the content in question, or at least make it unavailable.[49]

The sanction could be an adequate answer to the appearance and spreading of such websites like *pedomaci.hu*, which used to recycle images of underage children, uploaded to other websites (or social network websites), added titles and comments of a sexual nature, and published the images. The aim of the website, however, was not to cause damage to the victims (even if this is what they have achieved with their defamatory and privacy abuse activities), but to generate revenues from the advertisements placed on the website. The host provider of the website was a so-called anonymiser service provider, who guaranteed anonymity to all the uploaders of websites hosted by him. In 2009 and 2010, the hotline for reporting illegal contents and the police received several reports from the parents of children who featured in the images, because the website published these images without their consent, with defamatory, libellous, and humiliating comments. No criminal proceedings were launched because the public prosecutor's office ruled that the persons shown in the pictures waived their title to the images as personal data by voluntarily uploading those to (other, social) websites, as by doing so, they actively enabled anyone to freely dispose of the images.[50] The website's domain-name was removed by the registration authority, after it was called upon by Hungarian hotlines and civil rights organisations ,for the reason that the *name* of the website is in itself illegal, as it refers to the sexual exploitation of minors (*pedomaci* means "paedobear", where "paedo" stands for "child", and "maci" for "little bear"). At the same time, the host provider removed the offensive content at the request of the hotline. After that, however, the website was once more uploaded to the server of a host provider registered in the US with the web address pedomaci.net, and the website is still available today with a similar content and purpose.

Besides radicalisation, a liberal ridge is also discernible, according to which copyrighted material downloaded for private non-profit purposes and also the sharing of such material will be decriminalised in the new criminal code.[51] With this provision, Hungarian law-making trend makes a reverse turn and goes liberal. On 1 January 2011 the new Hungarian media law entered into effect, and gives the government the power to control the internet. Unlike previous legislation, it does not distinguish between traditional and new media as they are all subject to strict standards. According to critics, the new media law extends the protection against content, ranging from hate speech to unintentional insult and incitement to hatred. For content published on internet press outlets, websites and forums, the ISP is liable to the same extent as for services related to e-commerce (as a consequence, the forms of liability described in the E-Commerce Act apply to him). If he fails to remove offending content at the request of the victim, or the press supervision authority, then he will be held liable as if he was the content provider. Currently, however, there is no practice for settling debates arising from the media act.

There are many unresolved issues in relation to this example based on which we may say that the legal regulation of online abuse in Hungary still leaves a lot of loopholes, and therefore needs to be amended in the future whereas practice will be a consequence of court rules . It was civil rights organisations and hotlines for reporting illegal content that did the most to address the situation, which shows that informal self-regulatory

[49] Making electronic data terminally unavailable, Act 100 of 2012 Section 63 Subsection 1g.
[50] It is another fact however, that recycling personal data online does not include the users' consent to misuse their private information per se. We can witness a debate in Germany on similar grounds: In the statement of 14 July 2011, the federal government acknowledged the relevance and conduct of criminal investigations on social networking pages. According to the government's view, the pseudonymous participation of a covert investigation agent on a social networking website does not require a specific legal basis since there is no legitimate expectation of privacy on websites which do not require a verification of identity by registration. According to data protection concerns, it does not correspond to the constitutional requirements. See more: Drs. 17/6587 "Antwort auf eine kleine Anfrage der Fraktion 'die Linke'" (Drackert 2011).
[51] 2012. évi C. tv. 385.§ (5) bek.

measures are more suitable to cover the legal loopholes in disputes related to online contents.

NOTICE AND TAKEDOWN (N&TD) PROCESS AS A DECENTRALISED, EX-POST AND MULTI-ACTOR OPTION FOR REMOVING ILLEGAL INTERNET MATERIAL

How the definition of child pornography varies, is also demonstrated by the following campaign. In May 2009, a German user wrote to altogether 348 service providers all of whose contents were featured on the different publicly available European blocking lists. In the 12 hours following this email, ten service providers removed close to 60 depictions. However, 250 service providers replied that their inspections only revealed legal content.[52] This shows that there is a lot of content of disputed character that the users cannot access due to blocking. However, blocking does not delete illegal content which continue to be available, e.g. by technically bypassing the filter, or by subscribing to other (smaller or foreign) ISP not obliged to apply blocking measures.

The fight against illegal contents can only be successful if the content is removed from the host servers. This is promoted by the international network of hotlines,[53] which receives reports of illegal contents. The hotlines send an N&TD warning to the service provider, in which they request him to remove the illegal contents from his websites. We need to differentiate between N&TD procedures involving the direct and the indirect notification of the host provider. If the investigating authority informs the national hotline about the illegal content, thereafter the hotline turns directly to the ISP to have the content removed this makes the response significantly faster. INHOPE, the biggest international umbrella organisation of ISPs, accepts new members on condition that they subscribe to the N&TD principles of supporting investigating authorities and providing relevant and fast information. The original, so called indirect notification procedure did not use to involve the hotlines, so the police had to approach the individual ISPs in each case to get the contents removed. This was a significantly slower process in because the ISP judged the N&TD orders on a case by case basis. However, the new direct notification system involves the national hotlines in the notification chain and can skip the content verification. National hotlines must apply a special code of conduct developed by INHOPE (in 2010) for qualifying the content. Still, fastness and directness[54] could only be ensured after the European Commission in charge of the financing of the hotlines made it compulsory for hotlines in 2010 to apply N&TD, and the related best practices.[55] The network of hotlines is, as we see, a positive example of self-regulation. It ensures an informal system of contacts which approaches ISPs in accordance with standardised procedural rules developed for the coordination activities of INHOPE, and ISPs are then obliged to remove the content in question.[56]

Member States acknowledge and promote the significance of N&TD procedures in relation to a growing number of crimes. Accordingly, the Council of Europe's Cybercrime Convention managed to get a recommendation accepted as a separate act on the promotion of the self-regulation of harmful content, which encouraged user-level,

[52] Alvar Freude: Löschen statt verstecken: Es funktioniert! AK Zensur, 27 Mai, 2009 Available at: http://ak-zensur.de/2009/05/loeschen-funktioniert.html, accessed 12 October 2011.
[53] The biggest international hotline network is INHOPE established in 1999, which by now has a national hotline in 33 countries. Germany has been a member since 1999, Hungary since 2005. Currently, there are three hotlines in Germany and one in Hungary with a membership in INHOPE. For the list of INHOPE members see: https://www.inhope.org/en/hotlines/facts.html, accessed 12 October 2011.
[54] According to the 2010 statistics of INHOPE, N&TD procedures for ISPs in the same country or in an EU member state take about 12 to 36 hours, while the mean takedown time in the case of US-hosted material is approx. 24 to 48 hours. See: INHOPE Annual Report 2010 Available at: http://www.inhope.org/Libraries/Annual_reports/2010_Annual_report.sflb.ashx; [12 October 2011]
[55] For more see: http://www.inhope.org/system/files/INHOPE+BROCHURE.pdf and also http://www.cl.cam.ac.uk/~rnc1/takedown.pdf, accessed on 12 October 2011.
[56] On different N&TD regimes see: Moore & Clayton, 2008.

voluntary-based internet filtering, ahead of its time in 2001, including the labelling of websites, age verification system, and personal identification codes.[57] By contrast, a recent proposal (2010) to replace EU directive 2004/68/EC[58] would require Member States to ensure a unified compulsory blocking of all websites aimed at the sexual exploitation of children which has met some opposition. At the debate of the EU Civil Liberties Committee held on 12 January 2011, 11 out of 12 representatives were against making blocking compulsory for Member States. The arguments included that there is less and less static surfaces (websites) that can be blocked in practice, and that the disseminators of child pornography exchange their recordings less on the internet, and more on P2P networks, to which the blocking mechanisms are technically ineffective. And if the service provider still wants to make a website unavailable, this would immediately alarm the criminals, and would make the preparation of a successful action against them impossible.[59]

Applying the N&TD procedure would also make it possible for content providers (users, citizens) to be aware of their rights. One of the basic criteria for the rule of law is that regulations need to be transparent, based on which the consequences of citizen's behaviour are predictable, and the right to fair procedure, which is based on transparency and the right to objection (equal fighting chances principle). The introduction of the N&TD procedure – instead of blocking[60] – would make the processes not only more transparent, but also more efficient in the perspective of the courts' administration, relieving courts of a burden; the court would indeed need to examine only cases where the content provider raised an objection against the notice to remove the content. (Burkert 2000) At the same time, the general introduction of N&TD would likely encourage the *voluntary action of citizens* and altruism, which are the basis for the regulation of the internet. The internet cannot be regulated from the 'outside', by an external entity. It is the user community that can do the most for the 'cleanness' and legality of online content. For this, however, users should be able to inform themselves about the legality of the contents they publish. (Sieber 2000)

EUROPEAN AND GLOBAL TRENDS IN BALANCING CENTRALISED AND DECENTRALISED REGULATIONS

On the basis of the above we have demonstrated the functioning and the shortcomings of state regulated blocking measures and in contrast demonstrated how effective N&TD process can be: in particularly in cases of eliminating sexual child exploitation content. However, government based blocking has been applied in other sectors as well (e.g. copyright infringement) and as the following examples show self-regulatory measures (such as applying code of conducts to regulate illegal internet content) cannot function well without some form of central authorisation – stipulated by the state or the European Commission.

[57] Council of Europe Committee of Ministers Recommendation Rec(2001)8 of the Committee of Ministers to member states on self-regulation concerning cyber content (self-regulation and user protection against illegal or harmful content on new communications and information services) Available at: https://wcd.coe.int/wcd/ViewDoc.jsp?id=220387&Site=CM; accessed on 12 October 2011.
[58] Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA Brussels, 29.3.2010 COM(2010)94 final.
[59] On the public debate on EU wide blocking measures held in the Civil Liberties Committee on 10 January, 2011 see: EDRi-gram – Number 9.1, 12 January, 2011 Available at: http://www.edri.org/book/export/html/2491, accessed 12 October 2011.
[60] Stellungnahme: Aktuelle Berichterstattung zu „Löschen statt Sperren" Available at: http://www.eco.de/verband/202_8112.htm, accessed on 12 October 2011; Stephan Löwenstein: Löschen von Kinderpornos gelingt selten. Frankfurter Allgeimeine Politik. Available at: http://www.faz.net/aktuell/politik/inland/internetseiten-loeschen-von-kinderpornos-gelingt-selten-11008405.html, accessed on 12 October 2011.

Copyright regulation may provide a good example of these trends and their implications. France may not be a pioneer of government-level internet-control, but it is indeed the first EU Member State where internet blocking was introduced (maybe with the exception of the abovementioned German attempts to block illegal contents where the law never entered into effect). The so called HADOPI Act entered into effect in 2009 in France[61] prescribes a system of "graduated response" consisting of three steps (also called the 'French three strikes' against copyright infringement) under which the ISP has to give internet users downloading copyrighted material repeated warnings. If the first and the repeated warning produce no results, the users may be fined depending on the approval of a judge, or their internet connection may be suspended.[62]Modelling HADOPI, a similar sanction is to be introduced into the German Criminal Law in 2012, which will be a preliminary warning system (*vorgerichtliche Warnhinweismodell*) against illegal downloading practices of the user.[63] The warnings would be applied particularly against users of P2P networks, followed by the termination of the internet access of the user (*Zugangsperren von Internet*) consequently.

The U.S. introduced their Copyright Alert System in July 2011, which formulates unified regulations for the action by service providers against users committing copyright infringement (5 or 6 strikes law against copyright infringers). Service providers have had the practice of suspending the IP-addresses of those users committing mass copyright infringement for some time, but only at the express request of the victim. The current setup, however, works on the basis of a Common Framework, which unifies and partly automates the suspensions, and is based on a state-of-the-art system, which is also used in the fight against credit card fraud. Every bigger ISP joined the programme in the U.S., which ensures that blocked users cannot regain access to the internet by switching ISPs. In line with the policy, the service provider sends out electronic warnings to the users at the request of the beneficiary of the copyrights, and should this fail to bring results, as a last 'strike' he reduces the bandwidth of the user's connection, and may even suspend the IP-address of the rogue user, who will then have no internet connection at all. Parallel to the suspension, the service provider hands out the personal data of the offender to the copyright protection organisation, who will oblige the user to participate in a copyright "consultation". The Recording Industry Association of America (RIAA) as the initiator says that the programme primarily has an informative and educational purpose (as according to surveys the majority of users are not even aware that by downloading intellectual and artistic works they commit a crime), ISPs may join the programme voluntarily, and its most important goal is not punishment, but providing information, while they are still not obliged to monitor users.[64] Users' rights organisations on the other hand say that service providers were under pressure to join the programme, and the final – sixth – strike, the blocking of the IP-address is not only applied as a last resort, but at their discretion, as the Digital Millennium Copyright Act (DMCA) stipulates that the ISP has to give a warning of the possible suspension to the user. Should this be omitted, the DMCA terminates the safe harbour clause of the ISP,

[61] HADOPI: *Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet*, or "law promoting the distribution and protection of creative works on the Internet" Available at: http://www.senat.fr/dossier-legislatif/pjl07-405.html, accessed 12 October 2011.
[62] The United Kingdom passed a Digital Economy Act in 2010 that contained similar provisions.
[63] Ferner, J. (2012) Droht in Zukunft eine Sperre des Internetzugangs bei Rechtsverletzungen?, 3 February 2012. http://www.ferner-alsdorf.de/?p=6543; Staatssekretär Otto begrüßt neue Studie zur Bekämpfung von Internetpiraterie. Pressemitteilung 3: Februar 2012. www.bmwi.de/DE/Presse/pressemitteilungen,did=474200.html. See also Schwartmann et al. (2012) Vergleichende Studie über Modelle zur Versendung von Warnhinweisen durch Internet-Zugangsanbieter an Nutzer bei Urheberrechtsverletzungen – im Auftrag des Bundesministeriums für Wirtschaft und Technologie I C 4-02 08 15-29/11. Januar 2012. http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/Technologie-und-Innovation/warnhinweise-kurz,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.
[64] See Dave Parrack: U.S. ISPs agree to be copyright cops. TechBlorge, July 7, 2011 Available at: http://tech.blorge.com/Structure:%20/2011/07/07/u-s-isps-agree-to-be-copyright-cops/; [12 October 2011]

which means that the ISP can be held liable for the infringing activities of the user, as if he himself had committed those.

Organisations protecting the freedom of the internet and users' interests criticise this initiative and point out that it represents the interests of market actors one-sidedly.[65] The user only has the option of defence in the last phase – i.e. suspension – which may be particularly controversial as regards hospitality and catering outlets offering free wireless internet connections. The educational goal is compromised by the fact that the user is not referred to an independent and unbiased information website in the programme, but has to contact the copyright protection organisation (Centre for Copyright Information), which will obviously give priority to market interests over objectively informing the user.

Civil society groups emphasise that steps to control the internet by governments with the involvement of the ISPs are one-sided and forcible, and are only seemingly voluntary, as service providers would be turned into "quasi online policemen" by the measure. Service providers' organisations stand by the rights of ISPs and their users, and instead of protecting state or market interests, rather support total self-regulation, that is mainly the unified application of N&TD.[66]

We saw that the State can only carry out its controlling activities with the active involvement of service providers, which is the technical platform. In these relations, ISPs very often have no other choice but to cooperate with state or market-based interest groups. Otherwise they are not acquitted of the liability for user generated illegal content or illegal user activity. Online copyright debates shed some light to the correlation between market interests and the activities of ISPs. In 2011, the public prosecutor's office of Dresden launched a concerted raid against the German movie streaming platform Kino.to which involved house searches in several EU Member States of those publishing copyrighted material on the platform. The police seized the domain-name Kino.to, and several users who uploaded streams were disconnected from the web. Kino.to only provided the platform whereas the illegal activity, i.e. the copyright infringement, was carried out by the users. That being said, it is obvious that the operator of the platform had to be aware of the illegal activities of the users. The platform operator also generated revenues from the advertisements placed on the site. After the German raid, the biggest Austrian ISP UPC.at also blocked for public access to Kino.to based on a previous court order. At the time of the writing of this study, there are no final court decisions in any of the cases, but the trend is clearly outlined: to assert market interests, service providers are even willing to block websites offering a platform to illegal activities. Another example is the filter incorporated into Google's search engine service, which no longer offers the auto complete function for any searches including the string "torrent".

The following case sheds light on the cooperation of the state and service providers from a different angle. It shows that the measures and standards (code of conduct) of service providers introduced for their own quality assurance and smooth operation, and also consumer protection, cannot work without a contribution from the state and the support of the industrial sector. The content verification system was introduced by ISPs registered in Germany in 2003 (based on the German state's contract with ISPs for the protection of youth media). This basically meant the application of the PEGI system (Pan European Age Verification system), which verified the age and the type of media involved. Then in 2010, German internet content providers started verification on their

[65] Abigail Phillips: The Content Industry and ISPs Announce a "Common Framework for Copyright Alerts": What Does it Mean for Users? July 7, 2011 Available at: https://www.eff.org/deeplinks/2011/07/content-industry-and-isps-announce-common, accessed 12 October 2011.

[66] See for example Oliver Süme's claims against access blocking: Three strikes gegen filesharing. Abschalten ist unverhältnismäßig. Available at: http://www.taz.de/Three-Strikes-gegen-Filesharing/!75932/, accessed 12 October 2011.

own websites, but as the verification were not compulsory not all websites were involved, which made the system unreliable. Quality factors varied among the different German federal States (*Länder*), and in December 2010 the government took the new website-verification system designed by the ISPs off the agenda for political reasons. This is an example of how decentralised regulatory efforts cannot work without political and government support.

On the other hand, the decentralised regulation of N&TD has its own shortcomings as well. The process of removing illegal material by ISPs can differ service to service, so N&TD rules may be applied slightly differently. An example to this is the Newsbin2 case in the UK, where it has been shown that ISPs are very reluctant to remove illegal content or disable access to such material unless a court orders them to do so. Newsbin2 is a website providing links to a large amount of copyrighted material including films, music and computer games. The Newsbin2 precedent was set following a lengthy legal battle between the ISP and copyright holder film studios – including Disney and Fox – insisting that the service provider should remove the contents displayed, claiming that allowing users downloading their copyrighted material infringed their rights. The High Court ordered UK's biggest ISP to block its customers' access to Newsbin2 website and all other IP addresses or URLs that the operators of Newsbin2 may use.[67] This ruling was based on the Copyright, Designs and Patents Act in the UK which allows domestic courts to grant an injunction against an ISP to block access to the illegal content if the ISP had an actual knowledge of someone using its website for illegal purposes. Since the Newsbin2 injunction in 2011, the British Recorded Music Industry has also called the ISP to block access to Pirate Bay, a file-sharing website pursuing and allowing illegal activity to its users. However, the ISP has said it would only block access to Pirate Bay, if a court orders so.[68] Because the process of N&TD varies by individual cases and by ISPs, the EU Commission concluded in 2012, that a global resolution to this problem would be necessary to ensure consistency of the rules.[69]

CONCLUSION

Central (government based) internet blocking is applied first of all to filter out the most serious crimes – such as children's sexual exploitation – from the web. Governments turn to this central internet "cleansing" method in order to protect their citizens – and especially the most vulnerable group of society – from getting hurt and misused. Central level internet blocking requires rigorous obligations of cooperation on the Intermediary Service Provider's side. Since ISPs are responsible for providing access to, and hosting user generated contents on, the internet they can control the users' online activities, store (and provide) users' data to law enforcement agencies (on request). To conclude, ISPs are the practical executers of internet blocking. Nevertheless, this key position raises questions on ISPs' liability for user generated contents.

The EU clearly regulates the liability of ISPs. Case law of ECtHR, ECJ and the Member States also tend to exclude ISPs liability for user generated contents. Besides the fact that there is the interest of preventing serious crimes at risk, it is also important to understand the side effects related with surveillance (dataveillance) and the threats for liberties implied by government-based internet blocking regimes. The first significant shortcoming of central internet blocking is its improper technique of filtering out illegal

[67] [2011] EWHC 2714 (Ch) Case No: HC10C04385 http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWHC/Ch/2011/2714.html&query=Newzbin&method=boolean, accessed 21 September 2012.
[68] Sky follows BT in blocking Newsbin2. Out-Law.com 19 December 2011. Available: http://www.out-law.com/en/articles/2011/december/sky-follows-bt-in-blocking-newzbin2/; [21.09.2012]
[69] EU Commission will clarify website notice and takedown procedures. Out-Law.com 12 January 2012. Available: http://www.out-law.com/en/articles/2012/january-/commission-will-clarify-website-notice-and-takedown-procedures/, accessed 21.09.2012.

contents. It can over- and under-filter unrequested contents at the same time, meanwhile though, almost all blocking methods can be bypassed, and are therefore not truly efficient. Last but not least, blocking measures do not represent a solution, in the sense that they do not contribute to the repression of most serious crimes by law enforcement agencies. Top-down regulated blocking can be applied only with the side effect of infringing fundamental digital rights (free speech, free access to information and freely use of online applications is not illegal *per se*). It is not effective, and the necessity-proportionality criterion is, by contrast, easily compromised. 'While governments can play an *active* role in adopting legislation, promulgating guidelines or initiating education programmes, their role in self-regulation can be [only] characterized as *supportive* of measures (nominally) initiated by industry to avoid the heavier hand of regulation.' (Friedewald et al. 2009: 224) Self-regulatory measures such as research guidelines and codes of conducts can supplement governmental measures. They can be put in effect faster than centrally introduced measures that need to go through several bureaucratic hoops. While central regulative measures can be difficult to enforce, self-regulation is sometimes asymmetric and unbalanced. (Friedewald et al. 2009)

Bottom-up, ISP level regulation methods of internet blocking, serving on one hand the elimination of illegal web content and ensuring content quality on the other, work out positively not only by eliminating (removing) child exploitation contents but also other, less serious crimes such as copyright infringement. The internet is decentralized by definition, so that this network structure should be followed when sketching up filtering structures and solutions. The more actors we allow to join this "programme" (not only Government agents and the ISPs, but also ISPs' associations, the business sector and users' associations as well), the easier will it be to achieve our goal to select and eliminate illegal contents.

The expression "blocking" suggests that the internet can be easily and simply "cleared" of illegal content, but nothing is further from the truth. Internet blocking involves a complex technical process demanding contributions from *several stakeholders*. Internet blocking cannot be achieved properly (i.e. respecting the necessity-proportionality testes and also fulfilling technical punctuality) either by centralised or by decentralised regulation exclusively. The ideal solution requires a comprehensive and reciprocal *cooperation* between the stakeholders involved. If we look at the dynamics of top-down and bottom-up regulations in the world, we can see two *prima facie* opposite processes emerging. One is the effort of states to gain control over the internet, and thereby fight illegal online activities; a strategy which clashes with the activities of ISPs and civil society organizations, and who campaign for the unlimited and control-free development of the internet. The other trend involves the same direction; the increasingly closer intertwining of the two areas, the public and private spheres, but without a coercive measure of the state. Internet governance is the territory where public and private sector voluntarily cooperate.

In this article we have shed light to *the notice and takedown procedure* applied as a bottom-up, decentralized, ex post method especially successful in fighting online child exploitation. This is a plausible example of the *intertwinement of the state and the ISPs*, as even a well-developed decentralized regulatory measure can only create a unified, standard platform and achieve success in practice when governed and coordinated by a central body such as the ISPs' association (INHOPE) and the European Commission. Meanwhile, even the role of local law enforcement agencies is important in achieving the goals. While the state's efforts to implement internet-blocking cannot be realized without the active contribution of the ISPs, the opposite is also true: ISPs' regulatory mechanisms can only work properly with the political or financial support of the state and the market sphere. In the interest of ensuring the European principle of subsidiarity and improving efficiency indices, the state has to allow lower level regulatory solutions, whose evolution dates back to the birth of global electronic networks, and where the application promotes community crime prevention, the improvement of digital literacy,

user awareness, and the respect of fundamental digital rights. Our argument is that the notice and takedown procedure is currently one of the most refined and wide-spread form of these regulatory solutions used successfully in several countries in Europe. We can thus conclude that central regulation of internet blocking cannot provide full protection as it suffers from significant shortcomings, and, does not show respect to fundamental digital rights. Nevertheless, regulatory measures applied by ISPs are equally not eligible for eliminating illegal contents in themselves, when the state does not step up as an enforcing body.

***

REFERENCES

Albrecht, H-J. (2011). *Schutzlücken nach dem Wegfall der Vorratsdatenspeicherung,* Eine Studie des Max-Planck-Institutes für Ausländisches und Internationales Strafrecht. Available at: http://www.mpicc.de/shared/data/pdf/schutzluecken_vorratsdatenspeicherung_12.pdf. Last accessed 10 March 2013.

Burkert, H. (2000). 'The issue of hotlines' in J. Waltermann & M. Machill (eds.), *Protecting Our Children on the Internet*, Gütersloh: Bertelsmann Foundation Publishers, pp. 363-218.

Callanan, K., Gercke, M., de Marco, E. and Dries-Ziekenheimer, H. (2009). *Internet Blocking. Balancing Cybercrime Responses in Democratic Societies.* Aconite Internet Solutions, pp. 11-20.

Council of Europe Convention on Cybercrime of 23.11.2011 (CETS No.: 185).

Council of Europe Convention on the Prevention of Terrorism of 16.5.2005 (CETS No.: 196).

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25.10.2007 (CETS No.: 201).

Council of Europe Committee of Ministers Recommendation to member states on self-regulation concerning cyber content Rec(2001)8 (self-regulation and user protection against illegal or harmful content on new communications and information services) Available at: https://wcd.coe.int/wcd/ViewDoc.jsp?id=220387&Site=CM. Last accessed 12 October 2011.

Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism (O J L 164/3 of 22.6.2002) as amended by Council Framework Decision 2008/919/JHA of 28.11.2008 (OJ L 330/21 of 9.12.2008).

Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, [2004] OJ L 013, 20/01/2004.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems (OJ L 69/67 of 16.3.2005).

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), [2000] OJ L178/1.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [2002] OJ L201/37, 31.7.2002.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, [2009] OJ L 337/11, 18.12.2009.

Drackert, S. (2011). 'Die Verwendung fiktiver Indentitäten für strafprozessuale Ermittlungen in sozialen Netzwerken' *Eucrim*, 6 (3), pp. 122-127.

European Court of Justice, Case C-324/09, *L'Oréal v eBay*, Judgment of 12 July 2011, OJ C 269, 10.09.2011.

European Court of Justice, Joined Cases C-236/08 to C-238/08, *Google France, Google, Inc. v Louis Vuitton Malletier* (C-236/08), *Viaticum SA, Luteciel SARL* (C-237/08), *Centre national de recherche en relations* humaines (CNRRH) SARL, Pierre-Alexis Thonet, Bruno Raboin, Tiger SARL (C-238/08), Judgment of the Court (Grand Chamber) of 23 March 2010, [ECR 2010-2417].

Friedewald, M., Leimbach, T., Wright, D., Gutwirth, S., De Hert, P., González Fuster, G., Langheinrich, M. & Ion, I. (2009) Privacy and Trust in the Ubiquitous Information Society. Final Study Report (D4), prepared for the European Commission, DG INFSO, 27 March 2009.

Maier, B. (2010) 'How has the law attempted to tackle the borderless nature of the Internet?' *International Journal of Law and Information Technology*, 18 (2), pp. 142-175.

Magaziner, I. (2000). 'The role governments should play in Internet policy', in J. Waltermann and M. Machill (eds.), *Protecting Our Children on the Internet* Gütersloh: Bertelsmann Foundation Publishers, pp. 61-78.

Moore, T. and Clayton, R. (2008). 'The Impact of Incentives on Notice and Take-down' *Seventh Workshop on the Economics of Information Society (WEIS 2008)*, June 25-28, 2008. Available at: http://weis2008.econinfosec.org/papers/MooreImpact.pdf. Last accessed 12 October 2011.

Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA Brussels, 29.3.2010 COM(2010)94 final.

Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA Brussels, 29.3.2010 COM(2010)94 final

Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, [2009] OJ L 337, 18.12.2009.

Sieber, U. (2009). 'Sperrverpflichtungen gegen Kinderpornographie im Internet', *Juristen Zeitung*, 64 (13), pp. 653-662.

Sieber, U. (2000). 'Legal regulation, law enforcement and self-regulation: A new alliance for preventing illegal content on the Internet' in J. Waltermann and M. Machill (eds.), *Protecting Our Children on the Internet*, Gütersloh: Bertelsmann Foundation Publishers, pp. 319-400.

Tous, J. (2009). 'Government filtering of online content', *e-Newsletter on the Fight Against Cybercrime*, 1 (2), pp. 14-20.

Viola de Azevedo Cunha, M., Marin, L. and Sartor, G. (2012). 'Peer-to-Peer Privacy Violations and ISP Liability: Data Protection in the User-Generated Web', *International Data Privacy Law*, 2 (2), pp. 50-67.

Waltermann, J. and Machill, M. (eds.) (2000) *Protecting our children on the Internet* Gütersloh: Bertelsmann Foundation Publishers.