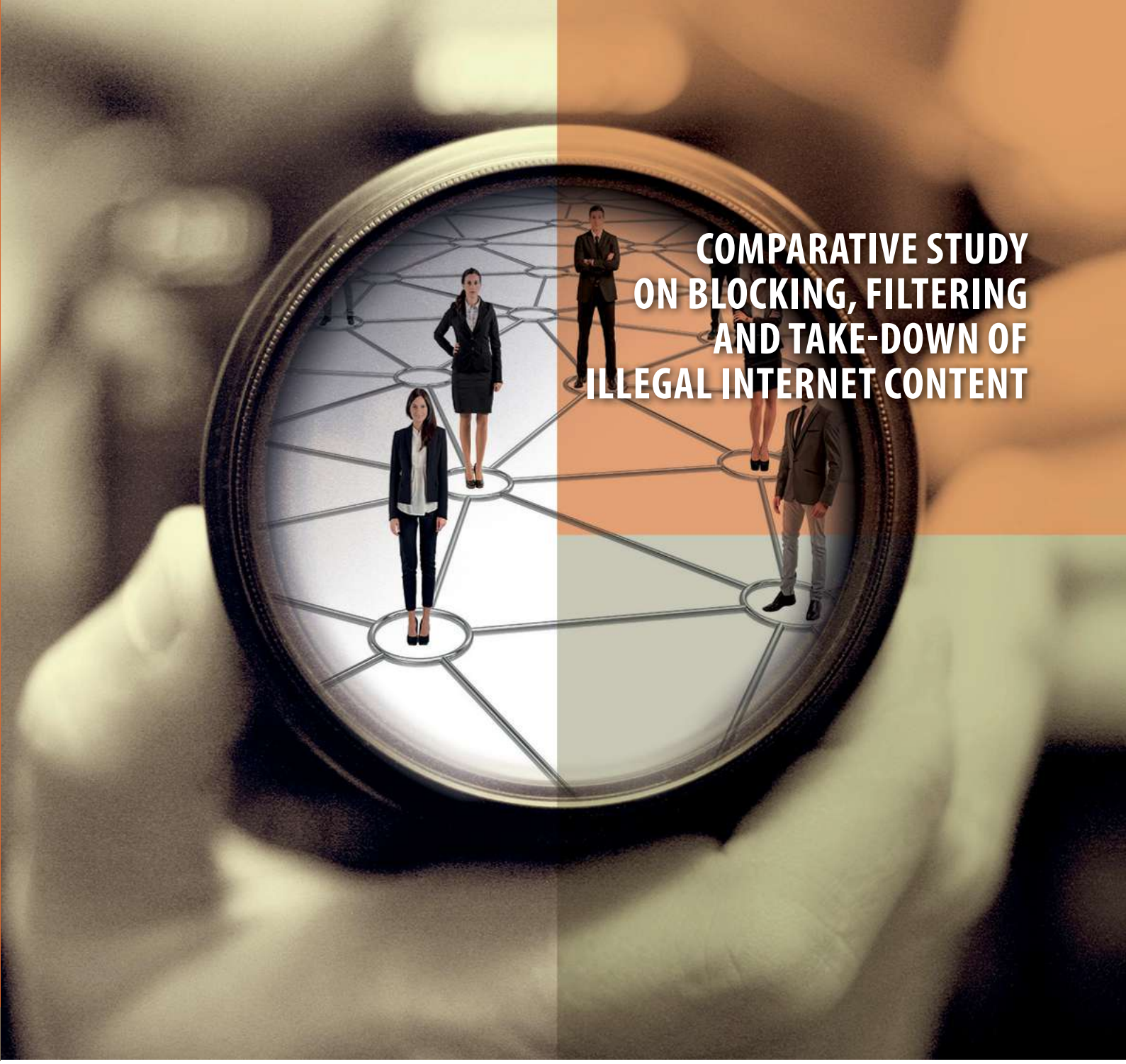

COMPARATIVE STUDY ON BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

www.coe.int/freedomofexpression

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COMPARATIVE STUDY ON BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Lausanne, 20 December 2015

Conseil de l'Europe

French edition:

Étude comparative sur le blocage, le filtrage et le retrait de contenus illegaux sur internet

Cover photo: Shutterstock

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Printed at the Council of Europe

EXECUTIVE SUMMARY

REGULATORY MODELS

Across the states examined, both the blocking, and removal of online material, are frequently treated in a similar way, and in countries with targeted legislative frameworks, they are often regulated under the same sets of rules. Two general categories of national regulatory 'model' have been identified.

First, there are **countries which do not have any specific legislation** on the issue of blocking, filtering and takedown of illegal internet content: there is no legislative or other regulatory system put in place by the state with a view to defining the conditions and the procedures to be respected by those who engage in the blocking, filtering or takedown of online material. An argument often put forward in this context is the impossibility for the legislator to keep up with the pace of technological developments. The underlying reasons for a lack of legislative activity may also be found in a country's legal traditions.

In the absence of a specific or targeted legal framework, **several countries rely on an existing "general" legal framework that is not specific to the internet** to conduct – what is, generally speaking - limited blocking or takedown of unlawful online material. This is witnessed in countries such as Germany, Austria, the Netherlands, the United Kingdom, Ireland, Poland, the Czech Republic and Switzerland. As such countries become increasingly confronted with the reality of internet-content-related disputes, the absence of legislative intervention has presented a challenge. In recent years, diverse mechanisms have been relied on to fill the regulatory gap and to address particular issues. Some jurisdictions have even chosen to combine approaches, maintaining a largely unregulated framework, but with legislative or political intervention in specific areas. In some jurisdictions, **self-regulation has been adopted by the private sector** to supplement the void left by the legislator's choice not to intervene in the area at stake. Other countries rely on **municipal courts** to ensure that the necessary balance between freedom of expression on the one hand, and safety of the internet and the protection of other fundamental rights on the other hand are preserved to the greatest extent possible.

Secondly, in many jurisdictions, the legislator has intervened in order to set up a **legal framework specifically aimed at regulation of the internet and other digital media**, including the blocking, filtering and removal of internet content. Such legislation typically provides for the legal grounds on which blocking or removal may be warranted, the administrative or judicial authority which has competence to take appropriate action and the procedures to be followed.

Whereas the more common **grounds for the adoption of blocking, filtering and takedown measures** are exhaustive and expressly defined in the legislation of most countries, which subscribe to such a regulatory model, certain jurisdictions have, in effect, extended the grounds on which blocking or removal may legitimately be taken – often by amendments to legislation or through creative judicial interpretation.

PROCEDURE

In relation to **child abuse material, terrorism, criminality (in particular hate crimes) and national security**, many of the states with targeted legal rules for the removal of internet content provide for the urgent blocking of such material without the need for a court order. Administrative authorities, police authorities or public prosecutors are given specific powers to order internet access providers to block access without advance judicial authority. It is common to see such orders requiring action on the part of the internet access provider within 24 hours, and without any notice being given to the content provider or host themselves. In other countries, such as Finland, where a court order is otherwise needed, hosting providers who have knowledge of such material may be expected to remove it voluntarily without judicial authority and to provide the content provider with due notice, which permits them to challenge the action through the courts.

A number of national systems require the relevant administrative authority to **obtain subsequent judicial approval of their order**, while others place a ***splash* page** at the location of the blocked material explaining why the material is blocked and how it may be challenged. In most countries, interested parties are given the **opportunity to challenge** blocking actions through usual criminal (or, where appropriate, civil) procedure laws.

Particularly in relation to material concerning child abuse and other serious crimes, many countries adopt a **"list" system**, whereby a central list of blocked URLs or domain names are maintained and updated by the relevant administrative authority. This is notified to the relevant internet access providers, who are required to ensure that blocking is enforced.

In many states, the takedown and blocking of material which **infringes intellectual property** and **privacy or defamation rights** is effected or authorised **pursuant to court order only**. Some countries have introduced alternative notice and takedown procedures designed to avoid the need for court action. In some countries, there is evidence of a procedure for rights holders to obtain removal of allegedly unlawful material, subject to content providers being afforded a due process to challenge removal. Particularly in relation to **defamatory material or content which otherwise infringes privacy rights** enforcement will usually depend on the initiative being taken by the person or organisation harmed, and so **many countries offer some form of 'notice and take-down' procedure**. These may require the person or organisation affected to notify the relevant website operator directly before procedures for taking down the material can be initiated. Where the website operator refuses to remove material determined to be unlawful, the relevant domestic authority may provide a deadline to the host to remove the material, and/or may leave itself exposed to third party liability for the content. Internet access providers can even be ordered to block access to the URL, or even the entire website.

CONSIDERATIONS RELATING TO FREEDOM OF EXPRESSION

When looking at the measures discussed in the context of freedom of expression, a **distinction** between blocking and content removal seems appropriate. The blocking, filtering or prevention of access to internet content are generally technical measures intended to restrict access to information or resources typically hosted in another jurisdiction. Such action is normally taken by the internet access provider through hardware or software products that block specific targeted content from being received or displayed on the devices of customers of the internet access provider. Takedown or removal of internet content, on the other hand, will instead broadly refer to demands or measures aimed at the website operator (or "host") to remove or delete the offending website content or webpages. Blocking is a very far reaching measure, whereas slightly different reasoning, mainly with regards to proportionality, applies to measures taken against a host with the aim of removal of internet content.

In the area of blocking, recent developments relate mainly to two main issues: voluntary blocking and the quality of the legal basis used for carrying out blocking measures. **Voluntary blocking** is especially problematic if (and given that) it is carried out without a legal basis and also raises serious due process concerns. In this context, it has been argued that states do not merely have a duty not to interfere, but must protect fundamental freedoms, and this especially in relation to access providers. It is interesting to note in this context that European Regulation 2015/2120 will not, as from 30 April 2016, allow voluntary blocking without a legal basis, including (as from 2017) blocking based on self-regulation.

The second issue is the **assessment of the legal basis** used for blocking measures under the criteria of Article 10 of the ECHR. Especially newly created legal bases, but also amendments to existing bases (or their application) need to satisfy the criteria put forward under article 10, namely whether the blocking is necessary in the democratic society to pursue a legitimate goal, as enumerated in Article 10(2) of the ECHR. The measure must also respect the limits of proportionality.

As to the **removal of content**, direct orders by state-authorities relating to removal by hosts of content need to satisfy the conditions of Article 10 (2) of the ECHR. This is true under both general and targeted national legal frameworks. However, the main issue in this context relates to the consequences of holding the host liable as a **co**-perpetrator, (at least if) he has knowledge of illegal content. The liability risk to the host might lead to over-removal. This tendency is best addressed by notice and take down procedures provided for by law. However, such provisions are (still) relatively rare. Self-regulated or voluntary notice and take down procedures, which are in place at least in certain areas in most states, often do not offer sufficient guarantees, especially from the due process perspective.

I. Introduction

On 24th November 2014, the Council of Europe formally mandated the Swiss Institute of Comparative Law ("SICL") to provide a comparative study on the laws and practice in respect of filtering, blocking and takedown of illegal content on the internet in the 47 Council of Europe member states.

As agreed between the SICL and the Council of Europe, the study presents the laws and, in so far as information is easily available, the practices concerning the filtering, blocking and takedown of illegal content on the internet in several contexts. It considers the possibility of such action in cases where public order or internal security concerns are at stake as well as in cases of violation of personality rights and intellectual property rights. In each case, the study will examine the legal framework underpinning decisions to filter, block and takedown illegal content on the internet, the competent authority to take such decisions and the conditions of their enforcement. The scope of the study also includes consideration of the potential for existing extra-judicial scrutiny of online content as well as a brief description of relevant and important case law.

The study consists, essentially, of two main parts. The first part represents a compilation of country reports for each of the Council of Europe member states. It presents a more detailed analysis of the laws and practices in respect of filtering, blocking and takedown of illegal content on the internet in each member state. For ease of reading and comparison, each country report follows a similar structure (see below, questions). The second part contains comparative considerations on the laws and practices in the member states in respect of filtering, blocking and takedown of illegal online content. The purpose is to identify and to attempt to explain possible convergences and divergences between the member states' approaches to the issues included in the scope of the study.

II. Methodology and questions

1. METHODOLOGY

The present study was developed in three main stages. In the first, preliminary phase, the SICL formulated a detailed questionnaire, in cooperation with the Council of Europe. After approval by the Council of Europe, this questionnaire (see below, 2.) represented the basis for the national reports.

The second phase consisted of the production of country reports for each member state of the Council of Europe. Country reports were drafted by staff members of SICL, or external correspondents for those member states that could not be covered internally. The principal sources underpinning the country reports are the relevant legislation as well as, where available, academic writing on the relevant issues. In addition, in some cases, depending on the situation, interviews were conducted with stakeholders in order to get a clearer picture of the situation. However, the reports are not based on empirical and statistical data, as their main aim consists of an analysis of the legal framework in place.

In a subsequent phase, the SICL and the Council of Europe reviewed all country reports and provided feedback to the different authors of the country reports. In conjunction with this, SICL drafted the comparative reflections on the basis of the different country reports as well as on the basis of academic writing and other available material, especially within the Council of Europe.

All through the process, SICL coordinated its activities closely with the Council of Europe. However, the contents of the study are the exclusive responsibility of the authors and SICL. SICL can however not assume responsibility for the completeness, correctness and exhaustiveness of the information submitted in all national reports.

2. QUESTIONS

In agreement with the Council of Europe, all national reports are as far as possible structured around the following lines:

1. What are the legal sources for measures of blocking, filtering and take-down of illegal internet content?

Indicative list of what this section should address:

- Is the area regulated?
- Have international standards, notably conventions related to illegal internet content (such as child protection, cybercrime and fight against terrorism) been transposed into the domestic regulatory framework?
- Is such regulation fragmented over various areas of law, or rather, governed by specific legislation on the internet?
- Provide a short overview of the legal sources in which the activities of blocking, filtering and take-down of illegal internet content are regulated (more detailed analysis will be included under question 2).

2. What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content blocked or filtered? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism);
  - the prevention of disorder or crime (e.g. child pornography);
  - the protection of health or morals;
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights);
  - preventing the disclosure of information received in confidence.

- What requirements and safeguards does the legal framework set for such blocking or filtering?
- What is the role of internet access providers to implement these blocking and filtering measures?
- Are there soft law instruments (best practices, codes of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

2.2. Take-down/removal of illegal internet content?

Indicative list of what this section should address:

- On which grounds is internet content taken-down/ removed? This part should cover all the following grounds, wherever applicable:
  - the protection of national security, territorial integrity or public safety (e.g. terrorism);
  - the prevention of disorder or crime (e.g. child pornography);
  - the protection of health or morals;
  - the protection of the reputation or rights of others (e.g. defamation, invasion of privacy, intellectual property rights);
  - preventing the disclosure of information received in confidence.
- What is the role of internet host providers and social media and other platforms (social networks, search engines, forums, blogs, etc.) to implement these content take down/removal measures?
- What requirements and safeguards does the legal framework set for such removal?
- Are there soft law instruments (best practices, code of conduct, guidelines, etc.) in this field?
- A brief description of relevant case-law.

3. Procedural Aspects: what bodies are competent to decide to block, filter and take down internet content? How is the implementation of such decisions organised? Are there possibilities for review?

Indicative list of what this section should address:

- What are the competent bodies for deciding on blocking, filtering and take-down of illegal internet content (judiciary or administrative)?
- How is such decision implemented? Describe the procedural steps up to the actual blocking, filtering or take-down of internet content.
- What are the notification requirements of the decision to concerned individuals or parties?
- Which possibilities do the concerned parties have to request and obtain a review of such a decision by an independent body?

4. General monitoring of internet: does your country have an entity in charge of monitoring internet content? If yes, on what basis is this monitoring activity exercised?

Indicative list of what this section should address:

- The entities referred to are entities in charge of reviewing internet content and assessing the compliance with legal requirements, including human rights – they can be specific entities in charge of such review as well as internet service providers. Do such entities exist?
- What are the criteria of their assessment of internet content?
- What are their competencies to tackle illegal internet content?

5. Assessment as to the case law of the European Court of Human Rights

Indicative list of what this section should address:

- Does the law (or laws) to block, filter and take down content of the internet meet the requirements of quality (foreseeability, accessibility, clarity and precision) as developed by the European Court of Human Rights? Are there any safeguards for the protection of human rights (notably freedom of expression)?

- Does the law provide for the necessary safeguards to prevent abuse of power and arbitrariness in line with the principles established in the case-law of the European Court of Human Rights (for example in respect of ensuring that a blocking or filtering decision is as targeted as possible and is not used as a means of wholesale blocking)?
- Are the legal requirements implemented in practice, notably with regard to the assessment of necessity and proportionality of the interference with freedom of expression?
- In the case of the existence of self-regulatory frameworks in the field, are there any safeguards for the protection of freedom of expression in place?
- Is the relevant case-law in line with the pertinent case-law of the European Court of Human Rights?
- For some country reports, this section mainly reflects national or international academic writing on these issues in a given state. In other reports, authors carry out a more independent assessment.

III Comparative Considerations

INDEX

This section will introduce the most common national models of regulation for the blocking, filtering and take-down of illegal internet content, along with an analysis of their consequences for the freedom of expression.

Offering a **general overview of the main domestic regulatory frameworks** identified by the study, it will highlight the principal issues with respect to freedom of expression as well as facilitating understanding of the featured country reports. Although the observations and commentary provided are inspired by, and based on, findings in relation to each of the member states to the Council of Europe, reference will be made to the most relevant countries only, by way of example. Moreover, it has been revealed by the present research that while certain countries may be identified as falling into a particular category of regulatory 'model', the variety of principles, approaches and measures witnessed means that it is not possible, under the current mandate, to offer an exhaustive comparative commentary.

This **comparative summary is divided into two parts**: in the first section, the different identified models of approaches to the issues of blocking, filtering and take down of illegal internet content will be examined. The second part will consider these measures and assess their impact on freedom of expression.

It will be seen that the blocking and removal (or "takedown") of online material is frequently treated in a similar way by the states examined, or, under countries with targeted legislative frameworks, under the same sets of rules.

These terms should not, however, be conflated. References in this section to the **blocking, filtering or prevention of access to internet content** will generally mean technical measures intended to restrict access to information or resources typically hosted in another jurisdiction. Such action is normally taken by the internet access provider through hardware or software products that block specific targeted content from being received or displayed on the devices of customers of the internet access provider. This can be achieved through a number of techniques, including the blocking of the Domain Name System (DNS) or the Uniform Resource Locator (URL). **Takedown or removal of internet content**, on the other hand, will instead broadly refer to demands or measures aimed at the website operator (or "host") to remove or delete the offending website content or webpages. Both internet access providers and website hosts may be referred to as "internet intermediaries".

1. NATIONAL MODELS FOR THE REGULATION OF BLOCKING, FILTERING AND TAKE DOWN OF ILLEGAL INTERNET CONTENT

Two general categories of national regulatory 'model' have been identified from the research in relation to the blocking, filtering and take down of illegal internet content.

First, there are **countries which do not have any specific legislation** on the issue of blocking, filtering and takedown of illegal internet content, where such actions are regulated with reference to general legislation or are undertaken by other non-state or state actors. These will be examined in section 1.1.

Secondly, countries in which the **legislator may be said to have "intervened" in order to establish a legal framework** in which blocking, filtering and take down measures are executed. A variety of different approaches and tools have been identified among those countries which have established such targeted regulatory frameworks, and these will form the focus of section 1.2.

1.1. Blocking, filtering and takedown of internet content in the absence of a targeted domestic legislative framework

A significant number of countries have no specific legal framework aimed at the blocking, filtering and take-down of illegal internet content. In other words, there is no legislative or other regulatory system put in place by the state with a view to defining the conditions and the procedures to be respected by those who engage in the blocking, filtering or takedown of online material.

In the absence of a specific or targeted legal framework, **several countries rely on an existing "general" legal framework that is not specific to the internet** to conduct – what is, generally speaking – limited blocking or takedown of unlawful online material. This is witnessed in countries such as Germany, Austria, the Netherlands, the United Kingdom, Ireland, Poland, the Czech Republic and Switzerland. In these countries, the legislator has, in effect, chosen to refrain from introducing a targeted legislative framework for regulating measures which enable the blocking, filtering and takedown of internet content.

The extent to which there is a lack of regulation nevertheless varies from country to country. Moreover, **various reasons explain this deliberate lack of intervention** on the part of the state. In some jurisdictions including the

Czech Republic and Poland, it can be said that the legislator has decided that internet-specific situations can be regulated by provisions of a more general order – indeed, which were never expressly intended to concern online material. Another argument often put forward in this context is the impossibility for the legislator to keep up with the pace of technological developments.

The underlying reasons for a lack of legislative activity may alternatively be found in a **country's legal traditions**. Certain states, such as the United Kingdom and other common law countries examined as part of this study, have not adopted an overarching legal framework aimed at regulation of the internet, instead preferring to leave most issues to voluntary regulation through private sector cooperation. Other countries, such as the Netherlands, prefer to follow an approach where the courts develop pragmatic solutions to solve issues at stake. Switzerland, on the other hand, has until recently not felt any imperative to adopt specific provisions for the blocking, filtering and takedown of internet content.

Nevertheless, as such countries become increasingly confronted with the reality of internet-content-related disputes, the absence of legislative intervention has presented a challenge. In recent years, **diverse, and often novel, mechanisms have been relied on to fill the regulatory gap** and to address particular issues. Some jurisdictions have even chosen to combine approaches, maintaining a largely unregulated framework, but with legislative or political intervention in discrete areas.

In some jurisdictions, **self-regulation has been adopted by the private sector** to supplement the void left by the legislator's choice not to intervene in the area at stake. Many jurisdictions have encouraged the private sector to adopt and implement codes of conduct on the internet. Generally speaking, this approach is usually intended to complement a larger set of rules which form a specific legal framework on the blocking, filtering and takedown of illegal internet content. However, in some jurisdictions, such as the UK, the blocking, filtering and takedown of illegal internet content is largely achieved through private regulation either by way of the application of internet intermediary terms of use policies, or voluntary cooperation of the internet service providers – whether access providers or host providers – with the police and other authorities. This is accompanied by legislative rules in discrete areas, such as the removal of terrorist material and notice and takedown procedures concerning defamatory content. In other states, such as Switzerland, blocking measures for certain types of internet content are only implemented following a dialogue between the competent administrative authority and internet access providers.

Other countries rely on the **municipal courts** to ensure that the necessary balance between freedom of expression on the one hand and safety of the internet and the protection of other fundamental rights is preserved to the greatest extent possible. This is witnessed, for example, in the Netherlands, as well as, to a lesser extent, in Germany.

1.2. Blocking, filtering and takedown of internet content as part of a targeted domestic legislative framework

In many jurisdictions, the legislator has intervened in order to set up a **legal framework specifically aimed at regulation of the internet and other digital media**, including the blocking, filtering and removal of internet content. It has been identified that such legislation typically provides for the legal grounds on which blocking or removal may be warranted, the administrative or judicial authority which has competence to take appropriate action and the procedures to be followed. These elements will be examined in the present section.

1.2.1. Grounds relied on for the blocking, filtering and takedown of internet content

In countries where the legislator has chosen to establish a targeted legal framework, it will usually **define the specific grounds and conditions** upon which action to block, filter or takedown internet content may be executed. In several countries, the legislation balances the competing interests at stake ex ante and provides for a take-down or removal order in case a specific interest is violated (harm test). In other countries, the balancing of interests is left to the courts.

Generally speaking, the grounds relied on broadly correspond to the **interests protected under Article 10(2) of the European Convention of Human Rights** (ECHR), namely: the protection of national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, and the prevention of the disclosure of information received in confidence.

For present purposes, **four broad categories of legal grounds** for the adoption of measures of blocking, filtering and takedown of internet content have been identified: the protection of health or morals, including the fight against websites containing child pornography or illegal online gambling websites, the protection of

national security, territorial integrity or public safety, including counter-terrorism, the protection of intellectual property rights and the protection from defamation and unlawful treatment of personal data. Different states define hate speech in different ways, and they may fall into different categories of legal grounds depending on the country concerned.

The way in which states with such a legal framework list and define specific grounds and conditions for the blocking, filtering and takedown of internet content varies considerably however. Whereas the more common grounds for the adoption of blocking, filtering and takedown measures are exhaustive and expressly defined in the legislation of most countries which subscribe to such a regulatory model, certain jurisdictions have, in effect, **extended the grounds on which blocking or removal may legitimately be taken** – often by amendments to legislation or through creative judicial interpretation. Some examples will be referred to below, but the focus in this section will nevertheless be on the grounds and conditions commonly relied on by the countries examined.

1.2.1.1. Protection of public morals or health

The most common measures observed under the grounds of protection of public morals or health are those targeted at the protection against **child sex abuse and illegal online gambling**. Such grounds widely witnessed across the jurisdictions examined and for child sex abuse in particular can perhaps be attributed, among EU states at least, to the implementation of Directive 2011/92/EU on the combat of the sexual abuse and sexual exploitation of children and child pornography, replacing Council Framework Decision 2004/68/JHA.

Some jurisdictions, however, **go beyond the commonly observed grounds** under which blocking and takedown measures for the protection of public morals and health may be authorised. This is the case, for example, of the Russian Federation, where the distribution of information containing obscene language, (non-child) pornography, and so-called homosexual propaganda are also listed among the online material which may legitimately be the subject of blocking and takedown measures. Likewise, the Turkish legal framework permits blocking, filtering and takedown measures aimed at internet content containing obscenity, promoting prostitution or which facilitates the use of drugs.

(a) Child pornography

The restrictive measures adopted in relation to online child sex abuse include orders to block as well as to remove the offending material, depending on the technical possibilities and the authority with competence for ordering such measures. There are **considerable differences in the way in which such measures are implemented**.

In certain countries examined, such as Spain and Cyprus, it is the **courts which take responsibility for ordering the blocking of online child pornography material**. In some jurisdictions, such as Portugal, a hybrid system has been put in place: an independent administrative authority has been given the job of implementing temporary blocking measures before judicial authorisation is then sought from the courts.

In other countries, including Belgium and Italy, th**e public prosecutor or judge of enquiry (*juge d'instruction*)** plays an important role in the adoption of blocking or takedown measures. In Italy, the prosecutor must authorise the list of illegal content before blocking or takedown can proceed, whereas in Belgium, it is the prerogative of the public prosecutor or *juge d'instruction* to order blocking or takedown measures in the context of the relevant enquiry into the illegal content.

Other jurisdictions have implemented **administrative blocking by a state authority**: this is the case in the Russian Federation, Turkey and also in Albania, where the state internet Surveillance Authority may order such measures. France has adopted a hybrid system where the police department competent in the field of the internet may adopt blocking or removal measures for content relating to criminal offences concerning child pornography, under the supervision of an independent administrative authority in charge of guaranteeing freedom on the internet.

In other jurisdictions, such as Finland, certain internet intermediaries have a particular responsibility, **even in the absence of a court order**, to act upon their knowledge and to take action in relation to content that is obviously illegal, including child pornography.

(b) Illegal online gambling

In the field of online gambling, several countries provide for blocking and takedown measures in relation to online gambling websites which are not licensed in their jurisdiction. Whether to block or to takedown the relevant content will generally depend on the location of the host of the website concerned. In most countries, such **restrictive measures are taken upon the initiative of the state authority** competent to monitor the

activity of gambling. This is for instance the case in Belgium, France, Turkey, Russian Federation and Cyprus. The extent to which such administrative authority is independent from state organs remains unclear in many jurisdictions.

The **implementation of the relevant order** is taken through action by national internet access providers, whether as a result of a cooperation agreement with the state Surveillance Authority (as is the case in Belgium), as the result of a court order (such as in France and Turkey, where courts also have authority) or in response to an administrative order (as seen in countries such as Turkey, the Russian Federation and Cyprus).

1.2.1.2. Counter-terrorism and national security

Many of the countries studied have **specific mechanisms in place** for blocking or removing internet content which relates to terrorist activity or which otherwise may threaten national security. For those states with legal frameworks which expressly grant institutions the authority to order internet hosts and ISPs to take such action, the source of such legal rules is varied.

Certain countries, such as Turkey, Spain and France, list such matters in the categories of prohibited activities which feature in a **single piece of legislation specifically concerned with the blocking and removal of internet content**. Operative provisions which give relevant bodies the power to take action may be included in this legislation itself (such as in France and Turkey), or **may be found in criminal codes or other laws** in which the unlawful activity in question is more widely regulated (such as the Spanish Criminal Code).

Other countries have introduced **legislation directly aimed at counter-terrorism efforts** which include provisions for the blocking and take-down of such material. This may, as is the case in Russia, sit alongside other targeted legislation concerning the blocking and take-down of unlawful content, but serve to provide specific procedures in relation to the removal of terrorist material. However, even some countries which have no targeted legal framework for dealing with the removal of harmful internet material consider counter terrorism as meriting legislative regulation. This can be seen, for example, in the UK's Terrorism Act 2006, which contains specific take down and removal provisions.

Many countries adopt **broad definitions of the unlawful activities** in relation to which internet blocking measures may apply. Potentially terrorist material, for example, may be removed or blocked under wider provisions protecting "public order", "public safety" or "national defence", or, as is the case in Belgium, behaviour which "contradicts public morals"; others refer specifically to material which "incites or condones" act of terrorism. One country of note is the Russian Federation, whose Federal Act on Countering Extremist Activity identifies a wide range of activities described as "extremist" and for which associated internet content may be blocked or removed. Such "extremist materials" are very broadly defined and may include content related to terrorist activity, but also to "the abasement of national dignity" and "the making of mass disturbances".

It is common among the countries with targeted legislative frameworks that blocking or removal orders may be **issued both by designated administrative authorities**, and on the **orders of a relevant court of law**. This is the case in Russia and France, where relevant administrative authorities or police bodies in these states have powers to require the blocking or removal of offending material without the need for a court order. In Turkey, unlike blocking provisions in relation to other harmful internet content, even the Prime Minister and other government ministries may request blocking or removal in cases of emergency. Other legal systems, such as that in Spain, demand a court decision or judicial confirmation of the decision of the relevant administrative body before removal may take place.

1.2.1.3. Protection of intellectual property rights

In light of Article 8(2) of the EU's Information Society Directive, EU member states have implemented into domestic law **measures necessary for ensuring that rights-holders whose intellectual property rights have been infringed** can apply to domestic courts for injunctions against internet intermediaries to have offending material taken down or otherwise blocked. Specific legislative rules, usually incorporated into broader legislation on intellectual property rights, normally provide this judicial authority, even in countries such as the UK, Germany and Sweden, where there are otherwise no targeted rules on the blocking and takedown of internet content in general.

However, countries with legislative frameworks specific to the blocking and removal of illegal internet content often provide clear rules on the **safeguards to be taken into account when removal is considered**. For example, Spain's Intellectual Property Act provides for the removal and suspension of content which infringes intellectual property rights, but other legislation on information society services which specifically regulates the removal of internet content, sets out the norms, procedures safeguards which must be respected whenever restrictive measures are applied.

In countries with targeted internet blocking and takedown laws, there is also **more evidence of detailed specific rules aimed at online intermediaries on aspects of intellectual property rights** beyond copyright, such as patents and trademarks. Whereas courts in other countries must apply principles and procedures relating to the issuing of injunctions under general intellectual property laws, legal systems such as France and Finland operate specific rules in relation to restrictive measures against internet intermediaries in these branches of intellectual property law. Compared to material published in more traditional ways, such rules will typically recognise the peculiarities of online content, such as the role of the internet intermediary to the author of the material in question.

1.2.1.4. Protection of reputation and personal data

Individual or private rights are **defined and treated differently across the countries examined**. They may include protection of reputation or defamation, protection of personal data and other violations of personal privacy. Legal mechanisms for the blocking and takedown of such individual rights are varied, even among those countries with legal frameworks specifically providing for the removal of unlawful internet content.

In many countries, the removal of such internet content takes place **under general rules for punishing breaches of privacy or individual rights**. In others, the legal basis for removal may be found in **legislation or codes specific to the removal of internet content** which causes harm or damage to an individual or organisation. France is an example of a country which provides for both possibilities. Certainly among EU countries as well as parties to the Council of Europe Convention 108, implementation of the EU or international framework at the domestic level means that countries already have rules in place aimed, generally, at the removal of personal data which breaches data protection principles. These have been used to require online intermediaries to remove the content where they may be considered as data processors of the offending material.

Russia and Turkey are examples of countries which have implemented data protection and privacy rules **specifically adapted to the removal of online data**. These generally allow individuals to seek orders against website operators and internet access providers, requiring them to remove content which breaches data protection principles.

Defamation and other rights related to the protection of reputation are often treated as criminal or civil matters, or sometimes both. Orders to block the offending material may be issued by courts as part of respective judicial proceedings, but many countries now also provide for takedown and blocking injunctions to be issued against internet intermediaries independently of civil or criminal proceedings against the author of such material. These often afford procedures for a more rapid removal of material than those witnessed in usual court proceedings.

In most states, it is c**ourts of law which retain ultimate authority for ordering the removal and blocking of internet content** said to breach such privacy rights. This is the case for countries which operate specific rules on the removal and blocking of internet material as well as those with no targeted legal framework, where individuals must generally rely on injunctive relief from judges under general laws. However, in countries such as France, Russia and Turkey, one finds **administrative authorities with considerable powers** to request the removal of material which breaches privacy rights, particularly in the field of data protection. These may even have the right, in certain circumstances, to order an internet intermediary to remove or block access to offending material without prior judicial authority.

1.2.2. Procedural mechanisms

Across the countries examined, the procedures followed in relation to the blocking and removal of internet content are diverse, and vary according to the legal system and the nature of the material in question. It is nevertheless possible to observe a number of common practices.

In relation to **child abuse material, terrorism, criminality (in particular hate crimes) and national security**, many of the states with targeted legal rules for the removal of internet content provide for the urgent blocking of such material without the need for a court order. Examples of this can be seen in countries such as Russia, France and Turkey. **Administrative authorities, police authorities or public prosecutors are given specific powers** to order internet access providers to block access without advance judicial authority. It is common to see such orders requiring action on the part of the internet access provider within 24 hours, and without any notice being given to the content provider or host themselves. In other countries, such as Finland, where a court order is otherwise needed, hosting providers who have knowledge of such material may be expected to remove it voluntarily without judicial authority and to provide the content provider with due notice, which permits them to challenge the action through the courts.

A number of national systems require the relevant administrative authority to **obtain subsequent judicial approval of their order** (such as is the case in Turkey in relation to material considered to pose a threat to national security and public order), while others place a ***splash* page** at the location of the blocked material explaining why the material is blocked and how it may be challenged. In most countries, interested parties are given the **opportunity to challenge blocking actions through usual criminal (or, where appropriate, civil) procedure laws**.

Particularly in relation to material concerning child abuse and other serious crimes, many countries adopt a **"list" system** (such as France, Russia and the UK), whereby a central list of blocked URLs or domain names are maintained and updated by the relevant administrative authority. This is notified to the relevant internet access providers, who are required to ensure that blocking is enforced. Such **lists are updated on a regular, even hourly, basis and are periodically reviewed** to determine whether the blocking is still necessary or if the material in question has subsequently been taken down. In some countries, such as Finland, certain blocking orders may expire after a certain period of time unless criminal charges or civil action is brought in relation to the content.

In many states, the takedown and blocking of **material which infringes intellectual property** and **privacy or defamation rights** is effected or authorised **pursuant to court order only**.

Even in countries such as Spain which have an administrative authority with powers to demand the takedown of **material which breaches intellectual property interests**, judicial authority is required. Rights of appeal under usual civil (and, where appropriate, criminal) procedures may then be relied on to challenge injunctions. Some countries have introduced alternative notice and takedown procedures designed to avoid the need for court action. Under Finland's new Information Society Code, for example, a procedure for copyright holders to obtain removal of allegedly unlawful material has been established, subject to content providers being afforded a due process to challenge removal.

As to **defamation and privacy rights**, given that enforcement will usually depend on the initiative being taken by the person harmed by the material in question (the "victim"), **many countries offer some form of 'notice and take-down' procedure**. These may require the victim to notify the relevant website operator directly before procedures for taking down the material can be initiated. Where the website operator refuses to remove material determined to be unlawful, the relevant domestic authority may provide a deadline to the host to remove the material, failing which, internet access providers can even be ordered to block access to the URL, or even the entire website. Such rules can, for example, be found in Turkey and Russia.

In other jurisdictions, such as France and Monaco, inaction by the relevant internet intermediary upon being formally notified by the rights holder of potentially unlawful content can have consequences for the liability of the intermediary for the content as a third party. In France, a failure by a website operator to remove manifestly unlawful content in the field of intellectual property rights can result in joint liability. Similarly, in the UK, where there is no wider framework on the removal and blocking of internet content, website operators are denied protection from automatic liability for defamatory statements in any subsequent civil action in circumstances where they have failed to take action as part of statutory notice and takedown procedures.

2. HUMAN RIGHTS ASPECTS OF BLOCKING AND HOSTING

From the perspective of Article 10 of the ECHR, an order by a state authority or a judge against an ISP (or host) to effect blocking (or removal) is a clear interference with the freedom of expression. There are some judgements in which the ECtHR held that hate speech or expressions of extremely anti-democratic opinions fall outside the protection of 10 of the ECHR. Nevertheless, the ECtHR applied the test of Article 10 even to these extreme expressions in almost all situations.

To justify an interference under Article 10 of the ECHR (or, in other words, to avoid violation of the right protected by Article 10), three conditions must be fulfilled. First, there must be a sufficient legal basis under national law for the relevant measure ("prescribed by law"). Secondly, that legal basis and the particular measure must pursue goals necessary in a democratic society as enumerated by Article 10 section 2 of the ECHR (e.g. national security, health or morals, protection of the reputation or rights of third parties, protection of confidentiality). Thirdly, that legal basis in national law and the particular measure based on it must be proportionate.

In the following reflections, we will differentiate between blocking on the part of an ISP (internet Service or Access Provider) and removal on the part of a host (host provider; see also above, 1). Blocking is a very far reaching measure and from the perspective of human rights law, states should be very careful when resorting to this measure. A slightly different reasoning from the perspective of human rights applies to measures taken against a host with the aim of removal of internet content (see on this more in detail below, 2.2.1).

2.1 Blocking and filtering by ISP providers

2.1.1. Issues

Before entering into the subject matter, it is important to refer to the conclusions of the ***OSCE Report*** *on Freedom of Expression on the internet, Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet* (2011) [1].[2]

In terms of human rights, the OSCE Report identifies three issues.

> (1) The first one is **voluntary blocking**, i.e. blocking carried out by ISP either entirely on their own initiative or on the encouragement of authorities or governments (see above, 1.1)[3].
>
> "There is concern that voluntary blocking mechanisms and agreements do not respect due process principles within the states in which they are used. In the absence of a legal basis for blocking access to websites, platforms, and internet content, the compatibility of such agreements and systems with Article 10 of the European Convention on Human Rights is arguably problematic. Although the authorities' good intentions to combat child pornography, and other types of illegal content is understandable, in the absence of a valid legal basis in domestic law for blocking access to websites, the authority or power given to certain organizations and institutions to block, administer, and maintain the blacklists remains problematic. Such a 'voluntary interference' will be in breach of Article 10 unless the requirements of Article 10(2) are fulfilled, and the necessity for interference is convincingly established. The European Court reiterated the importance of freedom of expression as one of the preconditions for a functioning democracy. Genuine, "effective" exercise of this freedom does not depend merely on the state's duty not to interfere, but may require positive measures to protect this fundamental freedom. Therefore, a blocking system based exclusively on self-regulation or 'voluntary agreements' risks to amount to a non-legitimate interference with fundamental rights".[4]
>
> (2) The second issue is the **Article 10 test** of proportionality and pursuance of a legitimate objective:
>
> "It is recalled that the **courts of law** are the guarantors of justice which have a fundamental role to play in a state governed by the rule of law. In the absence of a valid legal basis the issuing of blocking orders and decisions by public or private institutions other than courts of law is therefore inherently problematic from a human rights perspective. Even **provided that a legal basis exists** for blocking access to websites, any interference must be **proportionate** to the **legitimate objective pursued**. Within this context, it is submitted that the domain-based blocking of websites and platforms carrying legal content such as YouTube, Facebook, Wordpress, and Twitter could be incompatible with Article 10 and regarded as a serious infringement on freedom of speech. Such a disproportionate measure would be too far reaching than reasonably necessary in a democratic society. The internet started to play an essential role as a medium for mass communication, especially through the development of Web 2.0 based platforms, enabling citizens to actively participate in the political debate and discourse. These platforms provide a venue popular across the world for alternative and dissenting views. Therefore, banning access to entire social media platforms carries very strong implications for political and social expression".[5]
>
> (3) The third issue concerns the particular effects of **prior restraint**, censorship and chilling effects:
>
> "State-level blocking policies undoubtedly have a very strong impact on freedom of expression, which is one of the founding principles of democracy. Blocking orders that are issued and enforced indefinitely on websites could result in 'prior restraint'. Although the European Court of Human Rights does not prohibit the imposition of prior restraints on publications, the dangers inherent in prior restraints are such that they call for the most careful scrutiny on the part of the court. This is particularly valid for the press as news is a perishable commodity and delaying its publication, even for a short period, may well deprive it of all its value and interest. The same principles also apply to new media and internet publications. It is argued that prior restraint and other bans imposed on the future publication of entire newspapers, or for that matter websites and internet content are incompatible with the rights stipulated in the European Convention on Human Rights. The Strasbourg Court requires the consideration of less draconian measures such as the confiscation of particular issues of

1. OSCE, Organisation for Security and Co-operation in Europe, The Office of the Representative on Freedom of the Media, *REPORT Freedom of Expression on the internet, Study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet in OSCE participating states*, 15 December 2011, see especially the parts on blocking, country reports for all OSCE-countries. Online: http://www.osce.org/fom/80723?download=true .
2. For other sources on blocking, refer to Sieber/Nolde, *Sperrverfügungen im Internet, Nationale Rechtsdurchsetzung im globalen Cyberspace?* (Schriftenreihe des Max-Planck-Instituts für ausländisches und int. Strafrecht, 2008). Messerschmidt, *Internetsperren und Menschenrechte*, http://publikationen. collaboratory.at/mri/internetsperren-und-menschenrechte/#_ftn26. There might be a publication very soon by Messerschmidt (thesis at the University of Vienna, expected to be published in the year 2016). However, the results of this thesis were not accessible in time for consideration in the SICL's study.
3. The most prominent examples are the United Kingdom, the Netherlands, Denmark, Sweden, Norway, Switzerland and Liechtenstein, see the OSCE Report, p. 145 and 150-169.
4. OSCE Report, p. 178, references omitted.
5. OSCE Report, p. 178, references omitted.

publications including newspapers, or restrictions on the publication of specific articles. Arguably, the practice of banning access to entire websites, and the future publication of articles thereof (whose content is unknown at the time of access blocking) goes beyond 'any notion of 'necessary' restraint in a democratic society and, instead, amounts to censorship".[6]

These categories and issues will serve as the basis of the following analysis of human rights in the context of internet blocking and removal. Given the prior work collected in the OSCE report, the analysis will focus on recent developments.

Concerning the issue of prior restraint (issue 3, above), very little development has taken place. The main problems continue to arise in respect of the issue of legal basis (issue 1, above) and some developments have occurred in respect of proportionality with legitimate objectives (issue 2, above). This summary will be formulated with express reference to the different sources (ECtHR, CoE documents, EU-Law).

2.1.2. The requirements for a legal basis for blocking and the European Court of Human Rights

2.1.2.1. The Yildirim decision of the ECtHR (2012): the clear need for a legal basis

The need for a legal basis for any blocking measure (already indicated above) was further developed by the ECtHR Chamber judgment in the case of *Ahmet Yildirim v. Turkey*, (18.12.2012[7]). In this case, the blocking of access to the applicant's website had resulted from an order by the Denizli Criminal Court in the context of criminal proceedings against the owner of another site who was accused of insulting the memory of Atatürk. The court had initially ordered the blocking of that site alone. However, the administrative authority responsible for implementing the order (the TİB) had sought an order from the court for the blocking of all access to Google Sites, which hosted not only the offending site but also the applicant's site. The court had granted the request, finding that the only way of blocking the site in question was to bar access to Google Sites as a whole. Although neither Google Sites nor Mr. Yildirim's own site were concerned by the abovementioned proceedings, the TİB made it technically impossible to access any of those sites, in order to implement the measure ordered by the Denizli Criminal Court.

The Court accepted that this was not a blanket ban but rather a restriction on internet access. However, the limited effect of the restriction did not lessen its significance, particularly as the internet had now become one of the principal means of exercising the right to freedom of expression and information. The measure in question therefore amounted to interference by the public authorities with the applicant's right to freedom of expression. Such interference would breach Article 10 unless it was prescribed by law, pursued one or more legitimate aims and was necessary in a democratic society to achieve such aims.

A rule was "foreseeable" in its application if it was formulated with sufficient precision to enable individuals – if need be, with appropriate advice – to regulate their conduct. By virtue of Law nº. 5651, a court could order the blocking of access to content published on the internet if there were sufficient reasons to suspect that the content gave rise to a criminal offence. However, neither Google Sites nor Mr. Yildirim's site were the subject of court proceedings in this case. Although the decision of 24 June 2009 had found Google Sites to be responsible for the site it hosted, no provision was made in Law nº. 5651 for the wholesale blocking of access as had been ordered by the court.

Nor did the law authorise the blocking of an entire internet domain such as Google Sites. Moreover, there was no evidence that Google Sites had been informed that it was hosting content held to be illegal, or that it had refused to comply with an interim measure concerning a site that was the subject of pending criminal proceedings. The Court observed that the law had conferred extensive powers on an administrative body, the TİB, in the implementation of a blocking order originally issued in relation to a specified site. The facts of the case showed that the TİB had had little trouble requesting the extension of the initially limited scope of the blocking order.

The Court reiterated that a prior restraint was only compatible with the Convention if a strict legal framework was in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses. However, when the Denizli Criminal Court had decided to block all access to Google Sites, it had simply referred to an opinion from the TİB without ascertaining whether a less far-reaching measure could have been taken to block access specifically to the site in question. The Court further observed that there was no indication that the Criminal Court had made any attempt to weigh up the various interests at stake, in particular by

6. OSCE Report, p. 179 and 25, references omitted.
7. Application no. 3111/10.

assessing whether it had been necessary to block all access to Google Sites. In the Court's view, this shortcoming was a consequence of the domestic law, which did not lay down any obligation for the courts to examine whether the wholesale blocking of Google Sites was justified. The courts should have had regard to the fact that such a measure would render large amounts of information inaccessible, thus directly affecting the rights of internet users and having a significant collateral effect.

The interference resulting from the application of section 8 of Law no. 5651 had thus failed to meet the foreseeability requirement under the Convention and had not afforded the applicant the degree of protection to which he was entitled by the rule of law in a democratic society. The Court also pointed out that Article 10 § 1 of the Convention stated that the right to freedom of expression applied "regardless of frontiers".

The effects of the measure in question had therefore been **arbitrary** and the **judicial review** of the blocking of access had been insufficient to prevent abuses. There had therefore been a violation of Article 10 of the Convention.

2.1.2.2. The Cengiz decision of the ECtHR (2015): the quality of the law

For those states which have enlarged their existing legal bases for blocking (see below, 2.1.4.2, and above, 1.2.1), the current problem seems to be that of how far the legal system may go with blocking measures, especially the delimitation of the criminal offences for which blocking may be ordered and/or effected. This question (issue 2, above: proportionality to legitimate objectives) could have been addressed in the case of *Cengiz and Others v. Turkey*[8] (1.12.2015).

The case concerned the blocking of access to YouTube, a website enabling users to send, view and share videos. The Court found in particular that the applicants, all academics in different universities, had been prevented from accessing YouTube for a lengthy period of time and that, as active users, and having regard to the circumstances of the case, they could legitimately claim that the blocking order in question had affected their right to receive and impart information and ideas. The Court also observed that YouTube was a single platform which enabled information of specific interest, particularly on political and social matters, to be broadcast and citizen journalism to emerge.

The Court observed that the blocking order had been imposed under section 8(1) of the Turkish Law no. 5651. The Court reiterated on that point that in its judgment in the case of *Ahmet Yildirim v. Turkey*, it had already found that Law no. 5651 did not authorise the blocking of access to an entire internet site (overblocking) on account of one of its contents. Under section 8(1), a blocking order could only be imposed on a specific publication where there were grounds for suspecting an offence. It therefore emerged that in the present case there had been no legislative provision allowing the Ankara Criminal Court of First Instance to impose a blanket blocking order on access to YouTube. The Court accordingly concluded that the interference had not satisfied the condition of lawfulness required by the Convention and that Mr Cengiz, Mr Akdeniz and Mr Altiparmak had not enjoyed a sufficient degree of protection. Based on such reasoning, there was no urgent need for further explanations by the court.

In the meantime however, the Turkish legislator has expanded the legal basis for blocking. This new legislation was not applicable in the Cengiz-case; it constitutes a legal basis for overblocking. The Court did not directly tackle the problem. However, Judge Lemmens refered to a missed opportunity in his concurring opinion:

> « Après avoir conclu que l'ingérence litigieuse ne répondait pas à la condition de légalité posée par le paragraphe 2 de l'article 10 de la Convention, la majorité a estimé qu'il n'était pas nécessaire de contrôler le respect des autres exigences de ce paragraphe (paragraphe 67 de l'arrêt). En principe, une telle approche se justifie. Toutefois, dans les circonstances de la présente affaire, je pense qu'il s'agit d'une occasion manquée.
>
> En effet, la disposition légale sur laquelle la Cour s'est prononcée, à savoir l'article 8 de la loi n° 5651, a entretemps été complétée par une disposition, l'article 8A, qui prévoit désormais expressément que l'accès à l'intégralité d'un site internet peut être bloqué (paragraphe 22 de l'arrêt). Le présent arrêt porte donc sur une situation qui, pour autant qu'elle concerne la base légale de la mesure incriminée, appartient largement au passé. Dans ces circonstances, il aurait été souhaitable, à mon avis, d'examiner si, indépendamment du fait que l'ingérence litigieuse n'était pas prévue par la loi, cette mesure poursuivait un but légitime et si, eu égard notamment à ses effets, elle était proportionnée à ce but (voir, pour une approche similaire, Kurić et autres c. Slovénie [GC], n° 26828/06, § 350, CEDH 2012.
>
> Certes, la Cour ne doit pas se prononcer in abstracto sur le nouvel article 8A (paragraphe 75 de l'arrêt). J'estime néanmoins que, si elle avait examiné, fût-ce par *obiter dictum*, la finalité et la nécessité de l'ingérence litigieuse, son arrêt aurait pu éclairer les citoyens et les autorités turcs sur les principes auxquels doivent répondre tant les applications de l'article 8 que celles du nouvel article 8A de la loi n° 5651. »

At the moment (mid-December 2015), it is not clear whether this case will be reviewed by the Grand Chamber of the ECtHR.

8. Applications nos. 48226/10 and 14027/11.

The question of legitimacy, necessity and proportionality is getting more and more important in those jurisdictions in which specific legislation is in place and is currently being expanded and enlarged. Many states are just beginning to put legislation in place. For these reasons, it is very important that the Article 10 test, in respect of the quality of the law, be applied to a specific case of blocking.

The principal hurdle to be surmounted by these expanding legislative measures will be that of their necessity in a democratic society for the achievement of legitimate goals. One of these goals may be the **protection of the reputation of the individual**. The main question waiting for an answer is the following: will the guidelines developed with respect to this issue in offline (print media) cases also be applied in online cases, or will the Court take into account the special danger created by internet publications and therefore allow more extensive restrictions to be applied online than it would allow in respect of the print media. The latter approach seems to have some support.[9] Whether or not the Court follows the same guidelines, it should be remembered that persons who contribute to shaping public debate have to face more criticism then others, be it on- or offline.[10]

2.1.3. Legal basis and voluntary blocking and the Council of Europe

The danger of voluntary blocking or suppression of information by private actors is of concern to the CoE. In respect of this problem, the **Committee of Ministers** formulated recommendations in 2011:[11]

"[The] companies concerned are not immune to undue interference; their decisions sometimes stem from direct political pressure or from politically motivated economic compulsion, invoking justification on the basis of compliance with their terms of service.

> 5. These developments illustrate that free speech online is challenged in new ways and may fall victim to **action taken by privately owned internet platforms and online service providers**. It is therefore necessary to affirm the role of these actors as facilitators of the exercise of the right to freedom of expression and the right to freedom of assembly and association.
>
> 6. Interference with content that is released into the **public domain** through these means or attempts to **make entire websites inaccessible** should be judged against international standards designed to secure the protection of freedom of expression and the right to impart and receive information, in particular the provisions of Article 10 of the Convention and the related case law of the European Court of Human Rights. Furthermore, impediments to interactions of specific interest communities should be measured against international standards on the right to freedom of assembly and association, in particular the provisions of Article 11 of the Convention and the related case law of the European Court of Human Rights".

Furthermore, the Council of Europe **Commissioner for Human Rights** published an issue paper in 2014 on "*The rule of law on the internet and in the wider digital world*".[12] That paper addresses voluntary blocking in the UK and Sweden. It states as follows:[13]

> "There are serious doubts as to whether a blocking system that effectively imposes a restriction on most ordinary people's access to online information will ever be in accordance with the rule of law when it is chosen and operated by private parties, in the absence of public scrutiny, in the absence of a democratic debate, in the absence of a predictable legal framework, in the absence of clear goals or targets, in the absence of evidence of effectiveness, necessity and proportionality, and in the absence, either before or after the system is launched, of any assessment of possible counter-productive effects.
>
> In addition, there is the question whether governments that encourage (or even just allow) such systems can claim not to be responsible for them, or for the restrictions on information that are the practical results of the systems, simply because those systems are not underpinned by law. In terms of international human rights law, states are responsible if, within their jurisdiction, there are systems in place that effectively restrict the freedom to seek, receive and impart information and ideas regardless of borders for most of its inhabitants. The fact that Article 10 of the ECHR only refers to interferences with this right "by public authorities" does not mean that the state can simply wash its hands of measures by private entities that have such effect – especially

9. E.g., Grabenwarter, *ECHR-Commentary*, 2014, Art. 10, no. 59: "The risk of harm posed by content and communications on the internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than threat posed by the press. Therefore the Court finds that the policies governing reproduction of material from the printed media and the internet may differ. Journalists must be able to use information obtained from the internet without fear of incurring sanctions" (referring to ECtHR, 5 May 2011, *Editorial Board of Pravoye Delo and Shtekel versus Ukraine*, No. 33014/05, § 63). However, this case only concerned reproduction of illegal material. It did not concern the blocking as such.
10. Benedek/Kettemann, *Freedom of Expression and the internet*, 2013, p. 91: On libel tourism and forum shopping states "need to apply offline free expression protection guarantees to online situations, even if these have to be developed in recognizance of the special impact internet publications often have".
11. Declaration of the Committee of Ministers on the protection of freedom of expression and freedom of assembly and association with regard to privately operated internet platforms and online service providers, adopted by the Committee of Ministers on 7 December 2011, at the 1129th meeting of the Ministers' Deputies.
12. CommDH/IssuePaper(2014)1 of 08 December 2014, available at http://www.coe.int/t/dghl/standardsetting/media/cdmsi/Rule_of_Law_internet_Digital_World.pdf
13. Ibid, p. 72 *et seq*.

not if the state de facto strongly encouraged those measures. In such circumstances, the state is responsible for not placing such a system on a legislative basis: without such a basis, the restrictions are not based on 'law'".

Many such blocking measures are contained in self-regulatory schemes and contract terms of the ISPs. The **Recommendation of the Committee of Ministers** on the free, transboundary flow of information on the internet of 1 April 2015 reminds ISPs that such self-regulation has to comply with human rights standards:

> "States should encourage, facilitate and support the development of appropriate **self-regulatory codes** of conduct so that all stakeholders respect the right to respect for private and family life, the right to freedom of expression and the right to freedom of assembly and association, in full compliance with Articles 8, 10 and 11 of the ECHR, with particular regard to the free flow of internet traffic".[14]

2.1.4. Developments within the EU on legal basis and voluntary blocking

2.1.4.1. The special case: copyright violations, the ECJ and national courts

In the area of copyright protection, the European Union legislature created Art. 8 sec. 3 of the Info-Soc-Directive,[15] under which an ISP can be regarded as a sort of "passive" co-perpetrator of **copyright violations.**[16] This affects a relatively large group of countries, namely the member states of the European Union. All the EU member states have since transposed this rule into national law. In the year 2014, the ECJ decided in its UPC Telekabel Wien decision[17] (also called "the kino.to case", in a preliminary ruling on a request from an Austrian court) that a copyright holder is entitled to an injunction against an ISP on the basis of the Info-Soc-Directive. The ECJ conducted a very thorough and **consequent human rights evaluation** in that case, taking into account all interested persons, perspectives and several different human rights. Thus, there is a legal basis for blocking measures for the concerned states in this area.

National judgments on this basis have followed and will continue to follow. For many of those national legal systems which already had blocking legislation in place, this decision did not change much, because their legislative provisions already mentioned copyright infringements. For national systems (as for example Austria and Germany) which had not recognised blocking measures at all, this development was difficult and called for the use of national legal sources that were not really apt for this purpose. Thus in Austria, the highest court did it's best to integrate such measures on the basis of an "Erfolgsverbot" within the law of civil enforcement.[18] Doubts remain, but the Austrian courts have refused to ask the ECJ again or to check the compatibility of their solution with the Austrian federal constitution. In Germany, the Federal Court decided very recently to use the so-called "*Störerhaftung*" (disturber's liability) as a basis for blocking orders. At the same time, the Court decided that blocking is to be subsidiary to other protective measures. So as to get a blocking order, a claimant first has to show what steps he already took to try to get the material removed.[19]

There have also been strong objections to this development introduced by the ECJ; especially lower German courts have refused to follow the ECJ's lead because of the limited effectiveness of blocking measures, which might be a problem, on the level of human rights, in terms of **proportionality** and transfer of judicial power to ISPs.[20] Even in this field of copyright infringements, the last word may not yet have been spoken.[21]

---

14. Recommendation CM/Rec(2015)6 of the Committee of Ministers to member states on the free, transboundary flow of information on the internet, adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies, under 3. Value of Self Regulation.
15. Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.
16. Article 8 section 3 reads as follows: "Member states shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right".
17. C-314/12 - UPC Telekabel Wien. Judgment of the Court (Fourth Chamber) of 27 March 2014. *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft mbH*.
18. Refer to the Austrian national contribution to the present study, at point 2.1. See also Angelopoulos, *Are Blocking Injunctions against ISPs Allowed in Europe? Copyright Enforcement in the Post-Telekabel Legal Landscape*, in GRUR Int. 2014, 1089: "The real negative effects of the decision are likely to **be limited to Austria** – most member states do not have procedural constructions comparable to the Erfolgsverbot. Indicatively, the issue was already considered last year by the UK's Justice Arnold in *EMI Records v. British Sky Broadcasting*, who found that since under UK law the courts must carefully consider **fundamental rights** and proportionality before any blocking order is made, the question would not apply to the UK courts".
19. BGH , 26.11.2015, I ZR 3/14; I ZR 174/14. See Becklink 2001774. For the time being (mid-December 2015), the judgment has not been published.
20. Nazari-Khanachayi, *Access-Provider als urheberrechtliche Schnittstelle im Internet*, *GRUR* 2015, 115, 120: „Gerade weil der EuGH die rechtsstaatlichen Anforderungen vollständig außer Acht gelassen hat, darf erwartet werden, dass betroffene Internetnutzer und/oder Access-Provider im Falle einer unbestimmten Anordnung den Gang zu den nationalen Instanzengerichten riskieren werden, um eine Vorlagefrage im Hinblick auf die Zulässigkeit der herbeigeführten Übertragung von (faktischen) Hoheitsbefugnissen auf einen privaten Marktakteur zu erwirken".
21. See e.g. Husovec/Peguera: *Much Ado about Little – Privately Litigated Internet Disconnection Injunctions*, in IIC 2015, 10: "these injunctions raise serious issues regarding their compatibility with the EU Charter of Fundamental Rights. Indeed, the possibility of effective injunctions of this kind which conform with human rights turns out to be very narrow. In other words, the Directive's provisions promise much, but if applied correctly, they deliver little".

As blocking is **not very effective** in general, states have already started to find new solutions, especially in the field of copyright. A sort of next-generation-blocking of copyright violations is to be found in France, for example, is currently the subject of litigation in Ireland and will probably soon be found in the legislation of many other countries. Under this approach, the copyright holders not only rely on classical blocking injunctions, but also try to force the ISPs to "block" (or at least extract payment of fees from) those of their clients who download protected material without payment. A customer has "**three strikes**" and then "he/she is **out**" (or has to pay fees for the download to the rights holder). As far as this results in exclusion from internet access, the approach is of course a problem on another level, namely access to the internet as a human right. Such an "interruption" of access by violating users is subject to the test of Article 10. Procedural remedies must be available and the interruption may last only for a very restricted period of time.[22] For example, as soon as the relevant fees are paid or the user issues a declaration that no more infringements will be committed, her access to the internet must be reestablished.

2.1.4.2. The EU and blocking in other areas

In all other branches of the law, the EU has maintained a passive stance on blocking. Some endeavors have been made to produce blocking rules to fight **terrorism** and **child pornography**), but these have produced no binding results for the member states.[23]

EU law does stipulate a liability privilege for ISPs in the **E-Commerce Directive.**[24] ISPs are not to be made liable in civil or criminal law for purely passively transferred information, even after having been given notice thereof.[25] Nor may they be obliged to monitor content. This does not however, prevent a court or administrative authority from requiring the service provider to terminate or prevent an infringement, in accordance with a member states' legal system (i.e. if national law specifically so provides). It may be thought that specific legislation foreseeing blocking measures is required. Many member states did not recognise that need at the time of the issuance of the E-Commerce-Directive (2001) and wanted to base blocking orders against ISPs on the simple illegality of the content.[26]

The **European Commission** is thinking about changing the E-Commerce Directive on this point (**Strategy for A Single Digital Market**[27]). This might include imposing a duty of care on all service providers.[28] However, it is rather unlikely that this will lead to a positive duty of ISPs to block content. It seems more likely that blocking legislation at the national level will be more important in this regard. And the EU has already taken some measures in respect of blocking.

---

22. See Benedek/Kettemann, *Freedom of Expression and the internet*, p. 75 *et seq*.
23. See the OSCE Report, p. 139 et seq. For the activities of the EU in the field of freedom of expression, see Benedek/Kettemann, *Freedom of Expression and the internet*, p., 152.
24. 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').
25. Article 12 E-Com-Dir.
26. E.g. the Austrian legislator wanted to "keep" blocking based on the rule on defamation in the Austrian Civil Code (see the legislative material as cited in Brenn, ECG, 2002, § 19 No. 3, p. 305, 307). However, the Austrian legislator did not see that the rule on defamation could serve as a basis on removal against the host, but not for a blocking against an ISP.
27. Communication from the Commission of the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions, *A Digital Single Market Strategy for Europe*, 6.5.2015, COM(2015) 192 final.
28. Ibid, pt. 3.3.2: "The principle, enshrined in the e-Commerce Directive, that internet intermediary service providers should not be liable for the content that they transmit, store or host, as long as they act in a strictly passive manner, has underpinned the development of the internet in Europe. At the same time when illegal content is identified, whether it be information related to illegal activities such as terrorism/child pornography or information that infringes the property rights of others (e.g. copyright), intermediaries should take effective action to remove it. Today the disabling of access to and the removal of illegal content by providers of hosting services can be slow and complicated, while content that is actually legal can be taken down erroneously. 52.7% of stakeholders say that action against illegal content is often ineffective and lacks transparency. Differences in national practices can impede enforcement (with a detrimental effect on the fight against online crime) and undermine confidence in the online world. As the amount of digital content available on the internet grows, current arrangements are likely to be increasingly tested. It is not always easy to define the limits on what intermediaries can do with the content that they transmit, store or host before losing the possibility to benefit from the exemptions from liability set out in the e-Commerce Directive.
Recent events have added to the public debate on whether to enhance the overall level of protection from illegal material on the internet. In tandem with its assessment of online platforms, the Commission will analyse the need for new measures to tackle illegal content on the internet, with due regard to their impact on the fundamental right to freedom of expression and information, such as rigorous procedures for removing illegal content while avoiding the take down of legal content, and whether to require intermediaries to exercise greater responsibility and due diligence in the way they manage their networks and systems – a duty of care".

2.1.4.3. The 2015 Regulation on Open internet Access

Very near the end of the period available for the preparation of the current study (end of November 2015), the EU enacted its **Regulation on open internet access.**[29] This instrument contains (in a slightly hidden way) provisions of relevance to blocking.[30] It upholds the non-monitoring doctrine of the E-Commerce Directive.[31] The new regulation will enter into force on 30 April 2016. Its basic approach is that every **blocking of content is explicitly prohibited**, except for the (more or less) narrow exceptions laid down in the regulation.[32] The first important point to be mentioned here is that simple voluntary blocking without any legal basis (especially voluntary blocking of legal material by ISPs) will be prohibited (Article 3, section 3, subsection 3 lit. a of the Regulation). This amounts to a **ban of non-legally-mandated blocking** and may **paradigmatically change the blocking** environment.

In general, so-called "self-regulatory schemes" may be operated only until 31st December 2016.[33] After that point in time, every blocking activity will need to have some legal basis, as explained in the "exceptions" set out in the Regulation.

The primary environment for these rules on blocking is competition law and administrative law (i.e. relations amongst ISPs and between ISPs and national authorities). However, the Regulation itself implants the right to open internet access into every contract between an ISP and its customers; providers of internet access services shall put in place transparent, simple and efficient procedures to address complaints of end-users relating to the rights and obligations laid down in Article 3 (ban on blocking). As a consequence, any consumer may complain about any non-legally-mandated blocking. In addition, the relevant **national surveillance authority** is empowered to examine blockings and pursue violations (Article 5 section 3). National law will lay down the penalties for violations of Article 3 (Article 6).

The new regulation takes a rather expansive approach to exceptions to the ban on blocking. The Regulation (unlike some national systems) does not itself contain a list of subjects suitable for blocking but refers mainly to **national laws**, **national "measures"** and "**other measures**" **based on law**. Some preparatory documents of the EP refer directly to copyright law and the kino.to judgment of the ECJ.[34]

The new regulation not only refers to national laws and measures, but also to **European Union law**. The requirement of compliance with Union law extends, *inter alia*, to compliance with the requirements of the Charter of Fundamental Rights (CFR) of the European Union in relation to limitations on the exercise of fundamental rights and freedoms. This means that national laws or measures on blocking must comply with the CFR. Most importantly, any measures liable to restrict those fundamental rights or freedoms may be imposed only if they are appropriate, proportionate and necessary within a democratic society and if their implementation is subject to **adequate procedural safeguards in conformity with the ECHR**, including its provisions on effective judicial protection and due process.[35]

It should be noted that recital 13 of the regulation mentions not only "measures" (such as a direct court order against an ISP) but also "other measures". This refers to any measures ensuring compliance with Union legislative acts or national legislation (for example, obligations of compliance with court orders or orders by public authorities requiring blockage of unlawful content). This might imply that there is no need for a concrete court order or decision requiring each act of blocking; the simple possibility that a court order (or decision) could be hypothetically issued in the circumstances seems to be a sufficient basis for blocking by an ISP. That conclusion is very important for the **procedural aspects**.

This new regulation imposes a sort of new legislative framework for blocking within the EU. However, the main question of what may be blocked, where and when, clearly remains under the very strong influence of **national laws** and national particularities, as described in the various national contributions to the present study. The regulation will not change anything in this respect.

The big game-changer is that some jurisdictions will face the need to revamp their **self-regulatory blocking schemes** (this applies to the UK and its internet Watch Foundation, to the Danish, Swedish and Norwegian[36]

---

29. Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union.
30. Interestingly enough, blocking is regulated between the discussion of a two-class internet and the ban of roaming for mobile phones. That can be regarded as surprising.
31. Recital 10. Indeed, it leaves the E-Commerce-Directive entirely unchanged.
32. Recital 12.
33. Article 10 Nr. 3
34. E.g., *EPRS, The EU rules on network neutrality: key provisions, remaining concerns*, November 2015, p. 4, 5 (http://www.paulruebig.eu/attachments/article/1445/EPRS_BRI(2015)571318_EN.pdf); in German language, with reference to kino.to: http://blog.lehofer.at/2015/07/offenes-internet.html .
35. For all see recital 13 and Article 3 Nr. 3 subsection 3 lit. a.
36. The new regulation has relevance for the EEA.

voluntary blocking of child pornography and to the rather weak Finnish legal basis for blocking of child pornography[37]).

According to text of the new regulation, all traffic will be treated equally, subject to strict and clearly identified public-interest exceptions based on law. The future in this field might therefore involve more removal orders against host providers (see below, 2.2) and international cooperation to achieve removal (e.g. INHOPE).

2.1.5. Assessment

There is considerable and clear case law of the **ECtHR** and several material, including recommendations of the **CoE** on the subject of blocking and the necessary legal basis for such measures. This material is supported by some convincing literature.[38]

2.1.5.1. Blocking not based on law

There are serious concerns in respect of **blocking without a legal basis**. Within the **EU**, such blocking, where it exists, may not be upheld after beginning of 2017. The new rules of the European legislative do constitute a new step on the way to an open internet. Even in serious cases, like child pornography blocking, the ISPs may not simply block without any specific legal basis. Relevant legal foundations would enable judicial intervention to prevent abuse. This is even more important in cases of blocking based on less serious grounds.

2.1.5.2. Enlargement of existing or passing of new legislation on blocking

states which already had **legal provisions** in place, tend to enlarge and extend these provisions, as e.g. Turkey or France. That will be a problem in future cases coming from Turkey, but probably also from other countries. These states increasingly restrict freedom of expression by these extensions of their legislation.

There are also many **new blocking laws** to be found in other states (e.g. Switzerland has a proposal for blocking for illegal gambling and in case of violation of copyright; in Germany there is a discussion on specific legislation for copyright,[39] Austria plans blocking of foreign gambling). In these states however, the legislatures tend to avoid **overblocking**, if possible, and that might differentiate them from Turkey.

2.1.5.3. Assessment of the quality of the legal bases

On the one side, it is accepted (and welcomed) that states increasingly base their blocking on specific laws. However, there should be limits on the grounds for which a blocking can be regarded as necessary and justified. Vague expressions such as extremism (Russia) or propaganda might not qualify for blocking because it might not be clear how these terms refer to a specific legitimate goal under Article 10 (2) of the ECHR. It would have to be spelled out more explicitly which form of extremism or propaganda is meant.

For **Switzerland** and **Liechtenstein** it has to be added, that some provisions on blocking only foresee "recommendations " for blocking issued by the authorities to the ISPs. This attempts to transfer the decision for the blocking from the public to the private sector and faces the same criticism as voluntary blocking (see below, 2.1.5.4).

The blocking of illegal foreign **gambling** sites is questionable, if a state encourages (or does not seriously prevent) extensive online gambling offers by national companies or has no particular addiction prevention measures in place at the national level. In such a case such blocking might not seem necessary in a particular democratic society. The same reasoning might apply as against the gambling monopolies in general, since the online blocking of gambling sites effects first and foremost foreign gambling sites and simply protects a state's monopoly system. One may refer to the relevant case law of the ECJ in this respect.

As a summary of these reflections on the increased production of specific legal bases for blocking, one may refer to the statement of Judge Lemmens in the recent Cengiz-case, as reproduced above: an assessment of the **quality of the relevant blocking laws** is essential. The blocking measure (provided for by law) must be necessary in the democratic society to pursue a legitimate goal as enumerated in Article 10 (2) of the ECHR and the measure must respect the limits of proportionality.

---

37. See in this respect the country reports the questions 5 of the country reports for those countries which execute private or voluntary blocking.
38. Just to mention as an example: Akdeniz, *To Block or Not to Block: European Approaches to Content Regulation, and Implications for Freedom of Expression*, in Azevedo Cunha/Gomes De Andrade/Lixinski/Fétaira (eds.), *New Technologies and Human Rights, Challenges to Regulation*, 2013, p. 47, especially the conclusions p. 70 et seqs.
39. Nazari-Khanachayi: *Access-Provider als urheberrechtliche Schnittstelle im Internet* GRUR 2015, 115, 120: The author develops ideas for a future development. The creation of a legal basis would be necessary (although he proceeds from the basis that the BGH would not use the disturber liability, what the court ultimately did), there should be a special enforcement unit, like e.g. the IWF in the UK, and until the legislator reacts, the IPSs have to take care of the problem in their standard contract terms.

2.1.5.4. Voluntary blocking

In the *Yildirim*-case (see above, 2.1.2.1), the European Court of Human Rights stated that a restriction on access to a source of information was only compatible with the Convention if a strict legal framework was in place regulating the scope of a ban and affording the guarantee of judicial review to prevent possible abuses.[40] However, it seems that even after this decision, the states that encouraged **voluntary blocking** just continued their practices. Many states consider their systems to be in line with it (point 5 of the national contributions): criticism of national law within the country on the basis of the *Yildirim*-case, seems rather scarce. The excuse that such blocking might only be directed against heavily criminal material is not convincing.

It can be no excuse for a state that voluntary blocking of (obviously) illegal material is done by private companies or individuals. Some mechanisms in international law establish a liability of the state for the human rights violations committed by private entities. One of these situations is the so called doctrine of "para-statal entities".[41] If cannot be excluded that this doctrine might also apply to the provision of internet access. states (like e.g. Switzerland, Liechtenstein with their recommendations rules, or the UK and the IWF) continuously encourage voluntary blocking without legal basis, eventual infringements of freedom of expression by private companies may be regarded as infringements by the state itself.[42]

This being said, there is a surprising fact: decisions of the ECtHR or national courts on blocking outside the field of copyright violations and from outside of Turkey seem to be not too frequent. The reason might be that in systems with voluntary blocking, there might be a lack of transparency of blocking measures. Another reason might be that in systems with law based blocking, the legislator often explicitly forbids overblocking. Or users simply do not have an interest to take complicated and costly **legal measures** against the blocking of particular information that can be found a bit later or on another web-page. This argument is surely true for all systems. The **lack of effectivity** of blocking is also a big promoter of freedom of information. The national surveillance authorities of most countries did not have an eye on illegal blocking or even seem to have organised the blocking themselves (like e.g. in Romania, Italy or Portugal).

As mentioned above, the **EU banned blocking without legal basis in late 2015** and at the very end of the elaboration of this study. There will be a remedy for users and control over ISPs by national authorities. One will have to wait if the further developments confirm this first evaluation of the very new EU-regulation on an open internet access. One also has to wait, if non-EU-states follow similar paths. The EU measures seem a promising way forward.

2.2. Removal of content by a host[43]

2.2.1. Removal and blocking: subsidiarity

Normally, the first measure would be a removal order against a host, if such host has its seat or residence within the territory of the state taking the removal measure. Such removal would end the dissemination of

40. N 64 of the Decision.
41. See Hessbruegge, *Human Rights Violations Arising from Conduct of Non-state Actors*, Buffalo Human Rights Law Review, Vol. 11 (2005), 21-88, reprinted in Clapham, Human Rights and Non-state Actors, 2013, p. 87, 119, 125: Many "countries have begun to outsource services traditionally provided by public authorities, for example the provision of electricity or water". Parastatal companies can be *de jure agents* of the state. The decisive factor is the performance of a public function. This doctrine is also applied (to a certain extent?) to freedom of expression and newspapers (see p. 127). The execution of all blocking measures should be regarded as a public function. In the case of blocking for copyright violations, this task is even foreseen in the law. Next to that the doctrine of de *facto agents* applies: "If the Government gives an instruction to the management that is motivated by political reasons, it is exercising effective control". This may apply to ISPs which are owned by the state or where the state has a substantial influence as an owner.
42. See the ECtHR-cases *Costello-Roberts v.UK* (247-C, ser. A, 1993: *Corporal punishment in a private school*) and *Van der Mussele v. Belgium* (70, ser. A, 1983: association of lawyers shall perform legal aid pursuant to Article 6 section 3 of the ECHR). In both cases the private associations acted on behalf of the state.
43. See in general: Verbiest/Spindler/Riccio/Van der Perre, *Study on the liability of internet intermediaries* (2007), available at http://ec.europa.eu/internal_market/e-commerce/docs/study/liability/final_report_en.pdf. It is amazing that the Spindler-study is still so much up to date in the year 2015. The main problems in hosting seem to have stayed the same over almost ten years, namely, who qualifies as a host, when does a host have knowledge (or when can a host be presumed to have knowledge) and who is entitled to give a notification (e.g. in hate speech cases: only public officials or also private persons). Further comparative material would be: Spindler/Börner (Hrsg.), *E-Commerce-Recht in Europa und den USA*, 2003; *Holznagel,* Notice and Take-Down Verfahren als Teil der Providerhaftung, 2013 (to US and German law, and with very interesting proposals for a NTD-procedure for German law); see also Berger-Walliser, *Die Haftung von Hostprovidern für Rechtsverletzungen durch Dritte: Vergleich der deutschen und französischen eBay-Rechtsprechung*, ZEuP 2011, 476; to the *Delfi-case* and for a possible reform of the existing privilege and up to date comparative observations, see Fötschl, *Das Haftungsprivileg des Host-Providers auf dem Prüfstand,* MR-Int 2015, p. 47. For many other comparative references see: Wang, *Development of Hosting ISPs' Secondary Liability for Primary Copyright Infringement in China – As Compared to the US and German Routes*, IIC 2015, 275, and Matulionyte/Nérisson, *The French route to an ISP safe harbor, compared to German and US ways*, IIC 2011, 55.

illegal information in the state ordering the measure and also in other states (where such information might not be illegal, which could constitute a problem for the freedom of information). However, at the outset, no state can be obliged to tolerate illegality in its territory and the spreading of such information can then only be continued from another state (where the information is legal).

This leads to the second measure described above (2.1), in this report, namely blocking. It is normally directed against foreign information entering from abroad. The difference between the two measures is more of a factual nature: removal can only be ordered against a host within the territory of the state ordering the measure; the blocking can be directed only against national ISPs and concerns foreign hosts and often foreign content providers. However, it can also be difficult to get hold of a national host. The content provider may be anonymous. Nevertheless, to avoid the problem of technical ineffectiveness of blocking (**proportionality**) one might see the need for a hierarchy between removal and blocking: it may only be ordered if the removal is practically or technically not possible or considerable efforts at removal did not lead to any success. Some states do support such **subsidiarity of blocking**, as e.g. the German BGH did in his recent blocking judgement for copyrights violations (see above A.4.1). Such reasoning can be supported from the perspective of human rights law in terms of **proportionality**.

From the human rights perspective, blocking should be rather banned or restricted to very severe cases. The removal of obviously illegal material at the source and by the host itself should be rather encouraged. The removal of material in case of doubts about the illegality should be subject to prior decision. The conditions and mechanisms for such removal should be as clear, precise and effective as possible.[44]

Because of the ineffectiveness of blocking, states tend to enforce national removal measures against hosts and try to agree upon international cooperation for **removal across borders** (e.g. INHOPE network against child sexual abuse material, online grooming, hate speech, protection of children online).[45] From the perspective of human rights law, these developments can be welcomed.

2.2.2. Three basic approaches to removal and their human rights implications

From a human rights perspective, an important question concerning removal is (like for blocking): what can be regarded as a **sufficient legal basis** under national law for a removal? Such removal is a restriction of freedom of expression and the Article 10-test applies (see above, 2.1, General introduction).

The SICL would differentiate three different systems according to their legal bases.[46] However, different models are mixed. The co-perpetrator model is often mixed with self-regulation (e.g. Germany) but such a mix also exists for the NTD-procedures and self-regulation (e.g. the UK, making special removal legislation only in particular fields and applying self-regulations next to it or allowing "wild" removal[47]).

2.2.2.1. The co-perpetrator model and the host provider privilege

The first approach can be called the **co-perpetrator model**. The main idea is that traditional rules on co-perpetrators in civil, penal and even administrative law can be used as a legal basis for ordering blocking or removal by a host. In these systems the logical underpinning is that a host qualifies as a co-perpetrator to the content provider. This model is extremely broad. It is often linked to the host provider privilege. This privilege is generally not restricted to specific content[48] but applies to every sort of illegal content.

However, the **E-Commerce** Directive did not itself stipulate such a co-perpetrator liability. If (and only if) national law so provides, the host may be regarded as co-perpetrator according to the national conditions. The main idea of the **host privilege** according to the E-Commerce Directive[49] is that any EU-member state only has to take care that there is no civil, penal or administrative liability for the hosts, if and in so far as the host has no actual knowledge of the illegal material (of whatever nature); after actual knowledge the host has to react in good time. If the ISP or host does not act, even though it had knowledge, it could be in all cases regarded

44. See the conclusions of the Freedomhouse report on the internet, 2015, p. 13: "Governments that had already greatly expanded their arsenal of tools for controlling the online sphere—by disrupting ICT networks, blocking and filtering content, and conducting invasive surveillance—are now strengthening their application of these methods. As blocking has become less effective, more governments have shifted to censoring content through removal requests or more forceful, coercive tactics". Source: https://freedomhouse.org/sites/default/files/FH_FOTN_2015Report.pdf .
45. http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/illegal-content.aspx.
46. This categorization only slightly differs from the Spindler report (who use codified NTD-Procedures, Self-regulation, co-regulation, p. 106).
47. See the UK country report at 2.2. et seqs.
48. However, Switzerland plans at the moment to enact a host privilege only for copyright violations. A more restricted host privilege also seems to be in place in the US (see e.g *Holznagel*, loc. Cit., p. 5 et seqs.).
49. Article 14.

as a co-perpetrator in the penal, administrative or civil sense, if national law (not European law) foresees or allows such consequences.[50]

There is evidence to suggest that such co-perpetrator rules in penal, administrative law and in civil liability rules are wide spread and well known to probably all legal **systems of the member states** of the EU and the CoE. Especially systems with general codifications (Penal Codes, Civil Codes, Administrative Procedural Codes) in these matters tend to have such co-perpetrator rules. However, for more factual reasons the case-law coming from these systems concentrates on matters comparable to the more restricted NTD-approach (namely copyright, defamation, hate speech). Rather many EU-national legislatives have "opted" for this model, maybe unconsciously. They simply formulated their host-provider rules very much along the lines of the E-Commerce Directive. But they did not enact a particular NTD-procedure. Examples for this approach are Germany and Austria.

The disadvantage of this approach are that there is lack of precise legal rules. This leads to the problem that the situation is unclear in practice. E.g., for the German Federal Minster of Justice hate speech shall be removed by the host. If not, the host is threatened with criminal liability.[51] For others, hate speech is primarily protected by the freedom of expression and might not simply be removed.[52]

2.2.2.2. Self-regulation

To address the possible violation of other fundamental rights, many states have opted for **self-regulation**. A very good and recent example is to be found in Germany's fight against hate speech in connection with the refugee crisis (Task force against hate speech).[53] Similar codes of conduct or codecs are found in many states.[54] In some states they even seem to have effects in court (e.g. Belgium and Netherlands[55]). However, in others they only have soft binding effects between the parties being part of the self-regulation, but have no binding force in disputes between a rights holder or defamed person and a host (or do not provide a solution in critical cases, e.g. in Austria[56]).

2.2.2.3. NTD-procedures provided for by law

The next model stems from the idea that co-perpetrator provisions (or jurisprudence) are not a sufficiently clear legal basis for removal measures to be carried out by a host. For such measures one would need very

---

50. The European Commission announced, in middle 2015, a reform on the law for service providers including host providers (see above, 2.1.3.2. on the "Strategy for A Single Digital Market". There are indications that the development will lead away from (negatively formulated) liability privileges towards a more positive formulated, precise NTD-procedure with differing procedural requirements and safeguards according to the content that should be taken down (e.g. more serious violations have to be taken down immediately by the host; in unclear situations, there has to be a prior decision of a court to safeguard freedom of expression; precise rules on standing in case of hate speech). If (and only if) such a new EU-NTD-procedure is strictly followed, the host will be rewarded with an exemption from liability.
51. Maas, *Loschpflicht fur Hasskommentare?*, ZRP 2015, 222.
52. Härting, *Loschpflicht fur Hasskommentare?*, ZRP 2015, 222: „Erst die Kenntnis von solchen Rechtsverstößen verpflichtet zum Handeln. Dies aber auch nur, wenn es tatsächlich um eine Rechtsverletzung geht (zB Volksverhetzung), nicht jedoch bei jedem beliebigen „Hasskommentar(").
53. The German minister of justice formed a special task force against hate speech that presented its measures in the middle December 2015 (*"Together against Hate Speech: Ways to tackle online hateful content proposed by the Task Force against illegal online hate speech"*), see http://www.bmjv.de/SharedDocs/Artikel/DE/2015/12152015_ErgebnisrundeTaskForce.html; The main results are the following:
"The participants of the task force are all guided by the conviction that there is no place for hate speech on social media. This must be countered by a united front between the business sector, civil society, and policymakers.
The participants of the task force are in agreement that all hate speech prohibited under German law shall be reviewed and removed without delay upon notification (*"nach Inkenntnissetzung"*). The companies represented on the task force have agreed on a series of best practices and objectives, … that should guide internet companies in ensuring expeditious and effective processing of reports concerning illegal content, or content that is in breach of a company's terms and conditions, while also ensuring close collaboration in this regard with the organisations of civil society.
Freedom of speech is of vital importance to the democratic process. It protects all legitimate expressions of opinion, even if they are objectionable. All social actors are called upon to firmly face down racist propaganda and xenophobic prejudices. For this, counter speech is an effective instrument and civic engagement is called for. The companies and organisations of civil society represented on the task force stand ready to join forces to this end.
All measures to address hate speech should be considered in light of human rights. Stakeholders stress that freedom of opinion and freedom of expression are indispensable conditions for the full development of the person. They are essential for any society and constitute the foundation stone for every free and democratic society", http://www.bmjv.de/SharedDocs/Downloads/DE/Artikel/12152015_TaskForceErgebnispapier_eng.pdf?__blob=publicationFile&v=2
54. See the country reports under 2.2.
55. See the country report for the Netherlands, at 2.2: Even though the NTD-procedure can be regarded a form of self-regulation, non-compliance with the legal procedure will lead to civil or criminal liability placing the host under the formal regulatory framework.
56. See https://www.ispa.at/wissenspool/positionspapiere/ispa-position.html: „Für andere Kategorien vermeintlich rechtswidriger Inhalte (wie z.B. die unerlaubte Verbreitung urheberrechtlich geschützten Materials, Online-Glücksspiel, Diffamierung, Terrorismus etc.) stellt die Selbstregulierung nicht die ideale Lösung dar. Ein Provider ist nämlich nicht dazu in der Lage sich ein Urteil über die Rechtmäßigkeit oder Unrechtmäßigkeit derartiger Inhalte zu bilden". These statements were made for blocking, but apply also to hosting.

specific (new) laws and rules that do directly address hosts and make it very clear to them what they may and what they have to remove (and what not).

The best **examples** here are Finland,[57] Hungary,[58] Lithuania,[59] France,[60] Sweden[61] and partly the UK, where there are specific removal obligations only in particular matters (i.e., material encouraging terrorism, child abuse and obscene adult content, public order and targeted communications offences, defamation, confidential information).[62]

From the perspective of **human rights**, this model is a clear step forward. Such a NTD-system could, for the question of illegality of content, rely on the co-perpetrator model or could autonomously enumerate specific reasons for a take down. The latter model is more convincing. Indeed, these models regularly restrict considerably the amount and quantity of material that has to be removed. Not every illegality, like under the co-perpetrator model, can serve as a basis for removal. Very qualified reasons must be given. These models do, at the outset, comply with human rights standards. In addition, such specific regimes clarify the measures which a host may take out **of its own power** and the measures which it may only take after a court order or order by an administrative authority (as e.g. the surveillance authority).

2.2.2.4. Media law applied to hosts

It has already been mentioned that the co-perpetrator model has faced the objection that it is not sufficiently specific as a legal basis in terms of Article 10 of the ECHR. The co-perpetrator model seems to have also faced serious objections at the level of national substantive law. The first problem is that the application of co-perpetrator rules to hosts seemed very far reaching. Every sort of illegality could be pursued against a host. And this model is particularly harsh if serious criminal violations are under consideration (e.g. child pornography, nazi or terrorist propaganda). Courts in some jurisdictions were rather reluctant to regard hosts as perpetrators in this serious sense.

Some states (e.g. Russia, Poland, Hungry and Austria) have started to apply (all sorts of) their **media or press legislation** to hosts in their territory or created new Acts on Electronic Media with content similar to that of traditional media acts (e.g. Russia). Thus, the hosts are often characterized as publishers in the sense of press law. The hosts are also threatened with liabilities like a press company or publisher (**duties of care** for the content and specific content provisions, e.g. on defamation or hate speech[63]).[64] The reason for this development was mainly that the hosts were too inactive in removal of content or waited consciously for notices from third parties.

2.2.3. A human rights evaluation of hosting approaches

The basic principle should be that there are no differences of principle between **online and offline-cases**.[65] The mere fact, that one reaches a bigger audience online and one may cause bigger harm, should not directly and solely lead to different human rights evaluations.

---

57. There has to be a court order or a particular procedure for copyright infringement was followed. However, the host has to remove out of its own power the following material (after knowldge): hate speech (as regulated in the Criminal Code) or against making available a picture of child pornography, sexual violence or intercourse with an animal (see Section 184 of the 2015 Information Society Code, Finish country report, 2.2).
58. See the Hungarian country report, at 2.2.3.
59. See the Lithuanian country report, at 2.2.
60. See the French country report, at 2.2.
61. See the Swedish Act on bulletin boards, Swedish country report, 2.2.
62. See the UK country report at 2.2.1 to 2.2.5. However, such a specific regime should not allow "wild" removal next to it, as it does in the UK. See the UK country report, at 2.2: Although there are no other statutory provisions in either criminal law or civil law which provide for the removal of illegal internet content, it is reported that many hosts remove such material regardless of the legitimacy of the complaint, in order to better avoid being held liable
63. A very comprehensive comparative study on hate speech, media law and freedom of expression is: The European legal framework on hate speech, blasphemy and its interaction with freedom of expression, September 2015, PE 536.460.
64. It needs to be mentioned that by doing so, EU member states partly also started to **undermine the host provider privilege** and created obligations and liabilities for hosts that could go further than the E-Commerce Directive allowed, e.g. monitoring of content, abstaining from publication of problematic content, removal without or before notice). If such is the case, there are conflicting statements of the law and that is a problem on the basis of the element "prescribed by law" (as e.g. in the ECtHR-case of *Delfi*). However, as long as the duties of an online media company are interpreted in conformity with the host provider privilege (as e.g. for the time being in Austria (see national contribution, at 2.2. on the application of the Media Act to online media) there should be no obstacle to such an approach. It does not really help and it does no harm either.
65. See *Fatullayev against Azerbaijan*, 22 April 2010, application No. 40874/07. To this case, see the very instructive information in the country report for Azerbaijan. Also Benedek/Kettemann, *Freedom of Expression and the internet*, p. 88, 91, also to "libel tourism". For the particular case of social networks see Benedek/Kettemann, loc. Cit., p. 98.

2.2.3.1. Self-regulation

From the **human rights** perspective, this self-regulation faces the same criticism as blocking on a voluntary basis, namely that it does not constitute a sound legal basis ("prescribed by law") in terms of Article 10 section 2 of the ECHR.

Most importantly, self-regulation encourages over-removal. We see examples (e.g. in Poland[66] or in Norway[67]) where hosts started to remove what content ever out of their **own power** (wild "**over-removal**") to avoid risks. This risk is inherent to this model. Therefore, this model faces **human rights problems**.

2.2.3.2. The co-perpetrator model

As mentioned already above, the **co-perpetrator model** is strongly linked to the **host provider privilege** as adopted and practiced by many member states of the EU. The host provider privilege also contains a sort of **inherent human rights evaluation**. It is based on the idea that co-perpetrator rules (indirectly) lead to removal, because they might lead to punishing the ISP or host or to holding them liable (on the basis of actual knowledge or passivity). Otherwise a host simply would continue to commit the violation of law which could lead to further measures, maybe even up to a cancellation of the license of a host in a particular country. To the extent that a host is **obliged** to remove (to prevent liability), it also must be **authorized** to remove. To stop the co-perpetration, the host would have to **remove out of its own power**. In principle, according to the Directive, no court decision would be necessary to remove content. However, it does not explicitly say so. The second inherent human rights issue linked to the host provider privilege is that freedom of expression is given an extremely broad scope as long as the host is not notified. This is also a human rights reasoning enshrined in the host provider privilege of the E-Commerce Directive.

From the perspective of **Article 10 of the ECHR, the co-perpetrator model** might be rather problematic in terms of legal basis for a removal. These rules are not sufficiently **specific** to address the hosts directly. The basic assumption that the host may remove out of his own power might be problematic from the perspective of freedom of expression as well.

The **Article 10-test** in this respect refers to the national co-perpetrator rules in penal, administrative and civil law and the respective crime or tort committed by the content provider. In every single case, the test of legitimate goals must be applied. There might be many situations in which such rules would not pass this test. A singular substantive rule might be in line with the ECHR. But in combination with the co-perpetrator situation and "Article 10 of the ECHR, the test is a different and probably much narrower one.

From the perspective of **necessity** in a democratic society, legitimate goals and proportionality, there seems to be much less of a problem for removal than for blocking. The main cases on hosting concern copyright violations in Web 2.0 applications, defamation, libel, slander and hate speech. Copyright infringements constitute violations of "another person's right". As long as there is a **private person** individually offended, the legitimate goal will be "reputation of others". In hate speech and related cases one might think of "prevention of disorder" or "protection of morals". But here the lines of delimitations get very thin and notification might need to come from an authority.

That is especially true in **penal law**. The criminal character of **child pornography** or of **terrorist** material is clear. It is also clear that the content provider commits such a crime. However, it seems much less convincing that the host (or a media company reporting about such activities) commit such a crime as a co-perpetrator (even if they had knowledge of the content and stayed passive). Much depends on the national approach towards co-perpetrators and the requirements for their intention to commit such a crime. Systems may say that the omission by the host has to occur with the **intention** of actively supporting the content provider. Pure **laziness** or work overload might not be enough to designate the host as a co-perpetrator.

However, many EU-member states, in the course of the implementation of the EU-E-Commerce-Directive, created a general duty of the host to act after obtaining knowledge. By doing so, the host can commit any crime

66. See, e.g., the Polish country report, at pt. 2.2.1. on the consequences of the lack of a specific NTD-procedure: this situation causes an undesired **chilling effect** resulting in intermediary service providers disabling most content reported as potentially illegal in order to avoid any liability.
67. See the Norwegian report at 2.2.3: some hosts have devised **user agreements** that allow the host to remove any controversial content, including **content that is not illegal**, in order to protect themselves from liability in any controversy regarding content. By way of example, one author refers to an incident in February 2008 where the Norwegian host Imbera removed images of the Danish "**Muhammad cartoons**" from the websites of one of their customers, an organization called Human Rights Service. The grounds for the removal were that Imbera's user agreement prohibited users from uploading controversial content to Imbera's servers.

as a co-perpetrator. There remain serious doubts about whether such an approach should be followed.[68] To threaten a host with co-perpetrator liability in penal or civil law could lead to **over-removal**. However, it seems that have not been many cases in which a host would have really faced such consequences.

The very broad co-perpetrator principle has found a certain restriction. The main question is that of whether the specific material or comment is illegal. That can cause difficult problems of evaluation. For that reason, some national systems or national jurisprudence have restricted the obligation of the host to remove content out of his own power to cases of **"manifestly" illegal** material (e.g. the Belgian rules on hosting[69] or the new Finish rules on hosting, in Austria such restriction is found in case law). For other "normally" illegal material, further measures or a court order would be needed before removal.

2.2.3.3. Notice and take down-legislation

It is surely more appropriate to have in place specific **NTD-legislation** and specific rules on take down of specific material in place. From the perspective of human rights, it might even be necessary to install such a specific regime.

68. See to this point the country report for Azerbaijan on hosting and the relevant ECtHR material.
69. See No. 2.1. of the Belgian country report.

Across the member states of the Council of Europe, both the blocking and removal of online material are frequently treated in a similar way. However, the existence or the lack of a legislative framework specifically targeted to the internet, and the specificities of national regulatory "models" translate in different practices and can be a challenge for the states concerned.

The Council of Europe commissioned to the Swiss Institute of Comparative Law a comparative study in respect of filtering, blocking and take-down of illegal content on the internet in the 47 member states of the Organisation. This study describes and assesses the legal framework but also the relevant case-law and practice in the field. It comprises a comparative analysis – which is the subject of this publication – and country reports (available on the website: HYPERLINK "http://www.coe.int/freedomofexpression" www.coe.int/freedomofexpression).

PREMS 014017

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, 28 of which are members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE