Institut suisse de droit comparé
Schweizerisches Institut für Rechtsvergleichung
Istituto svizzero di diritto comparato
Swiss Institute of Comparative Law

COMPARATIVE STUDY

ON

BLOCKING, FILTERING AND TAKE-DOWN OF ILLEGAL INTERNET CONTENT

Excerpt, pages ii – iv

This document is part of the Comparative Study on blocking, filtering and take-down of illegal Internet content in the 47 member States of the Council of Europe, which was prepared by the Swiss Institute of Comparative Law upon an invitation by the Secretary General. The opinions expressed in this document do not engage the responsibility of the Council of Europe. They should not be regarded as placing upon the legal instruments mentioned in it any official interpretation capable of binding the governments of Council of Europe member States, the Council of Europe's statutory organs or the European Court of Human Rights.

Avis 14-067

Lausanne, 20 December 2015

Dorigny – CH – 1015 Lausanne - Tel : +41 (0)21 692 49 11 - Fax : +41 (0)21 692 4949 –
www.isdc.ch – info@isdc.ch

EXECUTIVE SUMMARY

Regulatory Models

Across the States examined, both the blocking, and removal of online material, is frequently treated in a similar way, and in countries with targeted legislative frameworks, it is 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, such as the UK and Albania, **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, such as the Netherlands and Germany, rely on the **domestic 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.

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. Finland, France, Hungary, Portugal, the Russian Federation, Spain and Turkey are examples of jurisdictions that have opted for this regulatory approach. 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 legal rules targeted at the removal of internet content provide for the urgent blocking of such material without the need for a court order in at least some of the areas mentioned. Greece, France, Portugal, the Russian Federation, Serbia and Turkey are examples.

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 (such as Turkey, in some cases) 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. The Portuguese regulation explicitly states so.

Particularly in relation to material concerning child abuse and other serious crimes or in relation to online gambling, many countries, such as France, Greece, Italy, Romania, the Russian Federation, Turkey and the UK, 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 Finland, for example, 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 seems not to allow voluntary blocking without a legal basis, as from 30 April 2016, 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 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) 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)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.