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 387-400

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
National reports current at the date indicated at the end of each report.

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

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 country 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. This phase was finalized in December 2015.

The Council of Europe subsequently sent the finalised national reports to the representatives of the respective Member States for comment. Comments on some of the national reports were received back from some Member States and submitted to the respective national reporters. The national reports were amended as a result only where the national reporters deemed it appropriate to make amendments. Furthermore, no attempt was made to generally incorporate new developments occurring after the effective date of the study.

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 country reports.

2. Questions

In agreement with the Council of Europe, all country 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 organized? 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.

LATVIA

1. Legal Sources

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

This topic is regulated, at least to some extent, by the Latvian legal system, as illegal Internet content is addressed in statutes and other legal acts described below. **International standards** have been transposed into the domestic regulatory framework, including the Convention on Cybercrime and Additional protocol to the Convention on Cybercrime, concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems,[1] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[2] and international standards of children protection.[3]

At the same time, there is no domestic legislation that specifically regulates the Internet or contains general provisions on blocking, filtering or removal of Internet content. Legal acts (statutes) that generally govern electronic communications contain some relevant provisions and legal acts which prohibit or obligate certain conduct generally also apply to the conduct online and may therefore result in blocking or filtering of Internet content. All in all, Latvian regulation of this field **can be described as fragmented**.

The following legal acts regulate blocking, filtering or taking down of the Internet content:

Electronic Communications Law (Sections 13 and 19 thereof are particularly relevant).[4] Section 13 of this Law was implemented by Governmental decree nr 291 of 9 June 2014, which regulates blocking of unlicensed on-line gambling websites.[5] **Personal Data Protection Law**[6] contains provision on removal of the content amounting to unauthorized personal data.

Other legal acts also apply:

Electronic Media Law[7] provides that defamatory or untrue information is to be removed from electronic media upon request by the affected person or when ordered by a court decision.

---

1 Adopted by Latvia and entered into force on 1 June 2007.

2 Adopted by Latvia and entered into force on 12 April 2001.

3 E.g., Convention on the Rights of Child (in force in Latvia as of 2 September 1990) and the Optional Protocol on the sale of children, child prostitution and child pornography (in force in Latvia as of 10 February 2006); Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (in force in Latvia as of 28 June 2014).

4 Adopted on 28 October 2004, in effect as of 1 December 2004. Unofficial translations of Latvian laws are available at http://vvc.gov.lv.

5 "Rules applicable to the Lotteries and Gambling Supervision Inspection to prepare and send the decision on the restriction of access to the interactive gambling organizers' Internet home pages which are not licensed inLatvia", Governmental decree (Cabinet of Ministers) nr 291 adopted on the 9 June 2014, in effect as of 1 August 2014 (unofficial translation).

6 Personal Data Protection Law, adopted on 23 March 2000, in effect as of 20 April 2000. The Inspectorate also Published Recommendations on the Processing of Personal Data on the On-line Social Networks, available at http://www.dvi.gov.lv/lv/latvijas-normativie-akti/metodiskie-noradijumi (07.08.2015).

7 Adopted on 12 July 2010, in effect as of 11 August 2010.

Criminal Procedure Law[8] and **Administrative Procedure Law**[9] do not regulate Internet blocking or filtering expressly but contain provisions that may, in principle, provide a basis for the blocking of websites or removal of Internet content.
The Law on Information Technologies' Security,[10] stipulates when a user's access to the electronic communication networks may be restricted.

Lastly, a **voluntary (self-regulating) memorandum** has been drafted by the non-governmental Latvian Internet Association which may be signed by Internet Service Providers (ISPs).[11]

2. Legal Framework

What is the legal framework regulating:

2.1. Blocking and/or filtering of illegal Internet content

As a starting point, the **law does not contain a list** of grounds to block or filter Internet content or specific requirements for such blocking or filtering, other than in the case of unlicensed on-line gambling sites.

Generally, online content that constitutes a **criminal act can be blocked or filtered**, however in practice such content rarely results in the blocking or filtering of websites or domains as such, but rather in removal of the illegal content. Criminal Law of Latvia envisages such offences as defamation,[12] racial and ethnic discrimination,[13] triggering national, ethnic or racial hatred,[14] public invitation to war or aggression,[15] acquittal and public glorification of genocide and crime against humanity,[16] as well as crimes against the State, including invitations to forcibly overthrow the government and change the political system,[17] invitations to destroy independence of Latvia[18] and invitations to destroy territorial integrity of Latvia,[19] invitation to terrorism and terrorism threats[20] and disclosure of State secrets.[21] Copyright infringements which cause significant damage to lawful interests are also punishable by criminal penalties.[22]

---

8 Adopted on 21 April 2005, in effect as of 1 October 2005.
9 Adopted on 25 October 2001, in effect as of 1 February 2004.
10 Adopted on 28 October 2010, in effect as of 1 February 2011.
11 Memorandum of Understanding between Net-Safe Latvia Center of Safer Internet, Information Technologies Security Incident Prevention Institution cert.lv and Electronic Communications Merchants on the Shaping of safe internet environment and combatting of distribution of materials containing criminalized pornography on the internet. Available at http://www.lia.lv/media/uploads/Saprasanas_memorands_informativi.pdf (09.08.2015).
12 Section 157 of Criminal Law, also envisaged in Civil Law, Section 1635.
13 Section 149.[1]
14 Section 78.
15 Section 77
16 Section 74.[1]
17 Section 80.[1]
18 Section 82
19 Section 83
20 Section 88.[2]
21 Sections 94 and 95.
22 Section 148.

Unlawful distribution of pornographic materials is also subject to administrative and criminal penalties.[23] In practice, combatting child pornography and other illegal pornographic materials online (such as zoophilia, necrophilia and sexual violence) appear to be the most common grounds for blocking or otherwise restricting Internet content.[24] At the same time, the objective of the prevention of a disorder or a crime which has not yet taken place is not, in itself, sufficient grounds to block Internet access or filter Internet content. It is necessary that illegal conduct has already taken place and criminal proceedings have been instituted. In one case reported in the media, the police took action to block a website on a Latvian server on suspicion of child pornography or a similar offence.[25]

Administrative infringements may also be grounds for blocking. As a specific example, **prevention of unlicensed on-line gambling and lotteries**[26] is a reason for blocking and corresponding criminal proceedings are not required to back up the blocking. Another example is the protection of **private sensitive data**.[27]

Offences such as copyright infringements, defamation and spreading untrue information about individuals and illegal publishing of personal sensitive data[28] would typically lead to the take-down and removal of the Internet content, rather than the blocking of a site.

Security concerns can be grounds for blocking user's access to electronic communications networks: section 9(1)(5) of the Law on Information Technologies Security stipulates that upon a request from the Institution on Prevention of Security Incidents, a user's access to electronic communication networks may be temporally restricted for up to 24 hours if the user substantially endangers the rights of other users, or the information system itself, or the security of the electronic communication networks. This Law does not, however, regulate the contents of the transmitted information.[29]

Specific requirements for blocking of the Internet content are only laid down in case of limitation on the access (blocking) of the webpage of an unlicensed gambling organizer. According to the Electronic Communications Law, such blocking requires a decision by the Lotteries and Gambling Supervision Inspection.[30] As specified by the Governmental decree issued on the basis of this Law,[31] the Inspection is to send an electronic request and the decision to the holders of the domain.lv and the Electronic Communications Merchant. The person whose rights are affected by such a decision

---

23 Administrative Violations Code, Section 173.[2], and Criminal Law, Section 166.

24 Law on Pornography Restrictions (adopted on the 3 May 2007, in effect as of 1 June 2007). Section 4 of this Law prohibits above-mentioned conduct. Also Section 6.3 and 7: Section 7 of the Law provides for the restrictions applicable to the distribution of pornographic materials in the electronic environment. It is also prohibited to advertise intimate services on the internet: para 6 of the Governmental Decree (MKN) nr 704 of 2 September 2008.

25 The site http://meitenes24.lv was a social project aimed at problematizing the youth sexual exploitation through the internet. The website was re-opened immediately after this had been clarified. Published in Latvian at http://www.diena.lv/sabiedriba/politika/prostitutu-internetveikals-ir-sociala-centra-marta-projekts-738726 (07.08.2015).

26 Article 46 and Article 74 of the Law on Gambling and Lotteries require that on-line gambling and lotteries' organizers receive a license in Latvia.

27 Administrative Violations Code, Section 204.[7]

28 Personal Data Protection Law, adopted on 23 March 2000, in effect as of 20 April 2000.

29 Section 2(2).

30 Section 13.1(2).

31 Section 13.1 of the Electronic Communications Law was adopted on the 11 November 2013 and entered into effect on the 1 June 2014.

may contest and appeal the decision according to the general procedures laid down in the Administrative Procedure Law.[32]

A legislative proposal is pending which would oblige the National Electronic Media Committee of Latvia to adopt a decision to block the home page of an unregistered Internet service supplier (this is relevant only to broadcasting services).[33]

In the event of the blocking of Internet content by the decision of the Data State Inspectorate (for example in the event of unlawful publication of **protected personal data**), the Inspectorate has the right to adopt a decision requesting the blocking or deletion of the data which was unlawfully made publicly available.[34] The Director of the Inspectorate or another official of the Inspectorate authorized by the Director may, *inter alia*, demand explanations from the relevant persons and inspect the (non-residential) premises in which the processing of data takes place.[35] The Law provides the right of the owner of the site or materials (i.e. addressee of the decision) to complain to the director of the Inspectorate and subsequently to the court, according to the general procedures laid down in the Administrative Procedure Law.[36]

Blocking of Internet sites and other content on grounds other than the two described above is not specifically regulated by statutes or other legal acts. However, general procedural safeguards laid down in the **Administrative Procedure Law** are usually available in cases where the public authority issues an administrative act.

The Administrative Procedure Law provides, *inter alia*, for the **right to submit a complaint** to the administrative institution which issued the contested decision (administrative act) and to appeal the decision to the administrative court, subject to certain procedural conditions. This Law also contains certain procedural rights for the complainant and a number of rules binding on the relevant administrative institutions. In addition, the applicant (complainant) may request that the Administrative court stop the effect of the contested administrative act until the ruling is adopted. However, in cases of sensitive data blocking, the law restricts the possibility to suspend the effect of the decision.[37]

In cases of blocking of Internet content in **connection with criminal offences**, there are **no special provisions in the Latvian law which would provide for requirements and safeguards to be met**. However, in practice, such blocking may only be requested by the state police in cases where the criminal investigation has been instituted, and in such a case, general safeguards envisaged in Criminal Procedure Law would apply, which are described further below.

The only provision of the Criminal Procedure Law which addresses electronic data is a provision on **storage of data of electronic systems** in Section 191, which requires Internet Service Providers and other similar entities or persons to ensure the storage, in an unchanged state, of the totality of the specific data necessary for the needs of criminal proceedings and to ensure the inaccessibility of such data to other users of the system.[38] The reference to the inaccessibility of data to other users of the

---

32 Section 77 et seq of the Administrative Procedure Law.

33 Status as of 30 July 2015. Information by the Ministry of Communications, project VSS-802 of 30 July 2015 available at http://tap.mk.gov.lv (08.08.2015).

34 Section 29(4)(3).

35 Section 30(1).

36 Personal Data Protection Law, Section 31.

37 Section 31(2).

38 Unofficial translation of Section 191 available at http://vvc.gov.lv.

system in Section 191(1) may indicate the relevance of this provision as a possible legal basis for blocking Internet content.

The legal basis for blocking can also be found in the provisions of Criminal Procedure Law regulating different procedural activities in the course of investigation and prosecution. Thus, this Law provides for a number of security measures to be imposed on the suspect,[39] including a **prohibition from specific employment** envisaged in Section 254. This section provides that a prohibition on specific employment is a restriction upon a suspect or accused, specified with a decision of a person directing the proceedings, from performing a specific type of employment (activities) for a time, or from execution of the duties of a concrete position (job). In practice, the prohibition of a specific employment has been used at least once to block access to a domain name. This specific example related to alleged copyright infringement.[40]

Another provision which may, in principle, be used is **seizure** and the procedures to be met in cases of seizure. The person directing the proceedings (the police) adopts a decision on the seizure. Although the provision does not mention anything about blocking (seizing) electronic content, these provisions might also be relied upon to block an Internet site.[41] In practice, this provision provides a basis for seizure of a server in cases where a website it hosts is suspected of containing unlawful information.

Both types of **security measures mentioned above may be appealed** within seven days to the investigating judge, but only if a person to whom a security measure has been applied may justify that the provisions of such security measure cannot be fulfilled.[42] An investigating judge may, with a decision thereof, reject a complaint or assign a person directing the proceedings to modify an applied security measure or the provisions thereof within three working days, or determine the amount of a bail. The decision of the judge shall not be subject to appeal.

In theory, the blocking or removal of Internet content can also be imposed in the judgment on the merits of a criminal case. Thus, the Criminal Law provides for restrictions of rights as a supplementary penalty precluding persons from "executing specific rights, taking up a specific office, performing a specific professional or other type of activity, visiting of specific places or events."[43] This restriction may, in principle, be applied by a court also in cases not expressly envisaged in the particular offences,[44] although it has not so far been used in practice.

It is also possible that blocking of Internet content will be requested by the police as a part of their operative activities. For example, **Law on Operational Activities**[45] provides that one of the police's operational tasks is the protection of persons against criminal threats and **preventing,** deterring and detecting criminal offences, including cases where no formal criminal proceedings have yet been instituted, possibly giving the grounds for blocking even where criminal proceedings have not been instituted. This Law does not contain any specific provisions on safeguards available to the persons involved.

---

39 Sections 243 and 254 of the Criminal Procedure Law.

40 Published at https://defense.lv/wp-content/uploads/2013/05/drosibas_lidzeklis_domena_blokesana.jpg (09.08.2015). The decision in question was issued in April 2013 and was reported by Nic.lv to be the first of this kind in Latvia.

41 Sections 186-188.

42 Section 262.

43 Section 44(1).

44 Section 44(3).

45 Adopted on 16 December 1994, in effect as of 13 January 1994, and Section 2(1)1.and 2 thereof.

The role of Internet Access Providers is, in general, a passive one, i.e. the actual implementation of the blocking or filtering measures initiated by a public authority. ISPs are not required to take active steps in this respect. In so far as blocking of unlicensed gambling sites is concerned, the Internet Access Providers[46] are obliged to implement any decision of the Lotteries and Gambling Supervision Inspection by restricting access to the website of the organizer of the interactive gambling which is not licensed in Latvia. The same obligation applies to the holder of the top level domain name .lv.[47]

In the field of combatting child pornography, a **voluntary agreement** (memorandum) has been drafted between Net-Safe Latvia[48] and Cert.lv,[49] on the one hand, and an Electronic Communications Merchant, on the other hand, in order to prevent illegal pornography (mainly, child pornography) more effectively.[50] The Draft (sample) memorandum published by Net-Safe encourages the Merchants to offer free filters to their customers, as envisaged by the Electronic Communications Law.[51] The Memorandum also envisages that Net-Safe, upon receiving permission from the State police, may inform the Merchants of illegal content so that they contact the owner of such content and ask the owner to remove the content. The memorandum does not expressly mention the blocking of Internet sites, nor the filtering or restriction of access to specific online content.

To date, there has not been any considerable amount of **case-law** directly addressing the issue of blocking the Internet in Latvia. One judgment deals with the application of the owner of a free gambling site to annul a decision by the Lotteries and Gambling Supervision Inspection which, *inter alia*, purported to restrict access to the site. The Administrative district court in Riga (first instance court) denied the application.[52] The court found that since the applicant's activities could be defined as on-line gambling within the meaning of the Law on Gambling and Lotteries, and no license was obtained as was required by this law, the decision of the Inspection was lawful. The case illustrates that administrative safeguards are in principle available in the case of blocking on this specific grounds.

Other than the case above, there are no court cases addressing the question of the legality of Internet blocking practices on their merits. In some criminal cases involving serious offences such as distribution of child pornography or ethnic or racial discrimination, the texts of judgments would usually mention **seizure of computers and other related equipment** but would not describe the pre-trial measures which may have been undertaken, including preliminary blocking of the relevant Internet content. There are no rulings in which a court has imposed blocking of an Internet site as a part of a criminal penalty.

2.2. Take-down/removal of illegal Internet content

Criminal Law of Latvia envisages such offences as defamation,[53] racial and ethnic discrimination,[54] triggering national, ethnic or racial hatred,[55] public invitation to war or aggression,[56] acquittal and

46 i.e. «Electronic Communications Merchants» in the Electronic Communications Law.

47 Section 19(1)(22) of the Electronic Communications Law.

48 Center of Safer Internet run by the Latvian Internet Association.

49 An entity for the prevention of information technologies security incidents and is run by the Agency of the University of Latvia "Mathematics and Informatics Institute of the University of Latvia».

50 Memorandum of Understanding between Net-Safe Latvia Center of Safer Internet, Information Technologies Security Incident Prevention Institution cert.lv and Electronic Communications Merchants on the Shaping of safe internet environment and combatting of distribution of materials containing criminalized pornography on the internet.

51 Section 19(1).17.

52 Judgment of 12 May 2015, Case nr. A420395614.

53 Section 157 of Criminal Law, also envisaged in Civil Law, Section 1635.

54 Section 149.[1]

public glorification of genocide and crime against humanity,[57] as well as crimes against the State, including invitations to forcibly overthrow the government and change the political system,[58] invitations to destroy independence of Latvia[59] and invitations to destroy territorial integrity of Latvia,[60] invitation to terrorism and terrorism threats[61] and disclosure of State secrets.[62]

Unlawful distribution of pornographic materials is also subject to administrative and criminal penalties.[63] Prevention of the processing of personal data in violation of the Personal Data Protection Law is an objective for take-down or removal of the Internet contents.[64] Protection of copyright is also an important ground.[65]

However, **express statutory provisions addressing removal or taking down of Internet content only include defamation, copyright infringement and protection of personal data**.

In so far as removal of illegally published personal data is concerned, Internet Access Providers must comply with a request by the Data State Inspectorate to remove such data from the web contents. The Personal Data Protection Law does not specifically address the role of Internet Access Providers but rather covers all persons and entities that process personal data. The Electronic Communications Law also contains specific rules addressing the obligation of the Electronic Communications Merchants with respect to the security of personal data. Online Merchants must ensure that personal data they collect is protected from unpermitted or unlawful processing, including (unlawful) disclosure.[66]

The **Electronic Communications Merchant** is also obliged to maintain proper internal procedures to protect personal data. More specific rules on such procedures are laid down by the Cabinet of Ministers.[67] These rules do not provide that the Merchant is entitled (or required) to block or filter the content containing sensitive personal data on its own initiative[68] but such a duty may be found in the provisions of the Personal Data Protection Law.[69]

The law does not contain any provisions on taking down or removal of Internet contens that would be addressed specifically to the owners of social media, social networks and other platforms. It has, however, been established in practice that the **Internet is subject to the same rules protecting copyright, prohibiting defamation, etc. as traditional media**. It follows that Internet host providers, social media and other platforms must perform the taking down or removal of Internet content upon the judgment of the court prescribing such a measure. Electronic Media Law also expressly requires

---

55 Section 78.

56 Section 77

57 Section 74.[1]

58 Section 80.[1]

59 Section 82

60 Section 83

61 Section 88.[2]

62 Sections 94 and 95.

63 Administrative LAPK Section 173.[2] and Criminal Law Section 166.

64 Personal Data Protection Law, adopted on 23 March 2000, in effect as of 20 April 2000.

65 Copyright law, Section 69(1)(7), 69(2)

66 Section 68.[1] of the Electronic Communications Law.

67 "Mandatory requirements to be observed when developing internal rules for investigation and prevention of infringements of personal data protection", governmental decree nr 627, adopted on 9 August 2011, in effect as of 18 August 2011.

68 Apart from the duty to analyse the risk related to processing of personal data before any changes in the processing of such data are made: para 5 of the decree (not relevant).

69 Personal Data Protection Law, adopted on 23 March 2000, in effect as of 20 April 2000.

that a media owner removes untrue information from the media upon the request from the affected individual or, if the media owner disagrees with such a request, by the court.[70]

Requirements and safeguards applicable to restrictions of Internet content in cases of personal data protection are laid down in the Personal Data Protection law which provides that administrative acts issued by an official of the Data State Inspectorate, or actual action undertaken by the official, may be contested to the director of the Data State Inspectorate. The administrative act issued by the director or the actual action by the director, as well as a decision regarding the contested administrative act or actual action may be appealed to a court in accordance with the procedures laid down in the law.[71]

A decision of the director or other official of the **Data State Inspectorate** regarding blocking of data, contesting and appealing of permanent or temporary prohibition of the data processing shall not suspend the operation of such decision, except in a case when it is suspended by a decision of a person examining the submission or application.[72]

In cases where the posting of the illegal content on the Internet has resulted in a criminal investigation, a **request by the police** is sufficient for the Electronic Merchant to remove the content in question. Criminal Procedure Law does not, however, contain any provisions giving specific procedural basis for the removal requests. General provisions on application of security measures may be applied. In such a case, the pre-condition is that criminal proceedings have been instituted in the case.[73] The legal basis for blocking or restricting the unlawful Internet content could also be derived from the **Law on Operational Activities** which contains some general provisions which may justify blocking or removing of unlawful Internet content.

In other cases not involving criminal offences, i.e. **copyright infringement and defamation**, it is necessary to obtain a court ruling to have the illegal content removed from the Internet. In copyright cases, it is also possible to request interim (provisional) protection measures to prevent the alleged infringement of copyright before the ruling on the merits has been issued. For such cases, the Civil Procedure Law envisages the possibility to apply to the court but these provisions apply to all cases, and not specifically to Internet.[74] The Civil Procedure Law also envisages a right to appeal the decision to impose interim measures.

As to the **soft law** on the removal of Internet content, in addition to the voluntary memorandum,[75] the Data State Inspectorate has published Guidelines on the principles of application of administrative fines to the sensitive data-related offences, which result in the removal of sensitive data from the Internet. However, the Guidelines do not deal directly with ISP practices on blocking or removal of Internet content.

The Latvian **court practice on the removal** of illegal Internet content is scarce. A judgment by the Administrative District Court in Riga (first instance court) addressed an application to annul a decision of the Data State Inspectorate in which the Inspectorate requested the applicant to remove a video

---

70 Electronic Media Law, Section 51.5.

71 Personal Data Protection Law, Section 31(1).

72 Personal Data Protection Law, Section 31(2)

73 See Question 2.1.

74 Civil Procedure Law, Sections 250.[11]-250.[14].

75 Memorandum of Understanding between Net-Safe Latvia Center of Safer Internet, Information Technologies Security Incident Prevention Institution cert.lv and Electronic Communications Merchants on the Shaping of safe internet environment and combatting of distribution of materials containing criminalized pornography on the internet.

from youtube.com.[76] The video in question, filmed by the applicant, contained images of **policemen** as well as their voices in police premises. The police sent a letter to the Inspectorate asking it to take action to have the video removed as incompatible with the Personal Data Protection Law. The court examined whether the Law protects officials in the given situation, i.e. whether their rights to private life could be protected. The court found that the Law applied in this case. Furthermore, the court pointed out that the Inspectorate's request to the applicant to remove the video (within five days) and send the evidence of the removal to the Inspectorate amounted to the imposition of an obligation to do so, and not merely a voluntary suggestion. According to the court, this request, which had a legal basis in a statute, was also proportional, legitimate and necessary. In particular, the Inspectorate only asked to remove the video from the Internet and not to destroy the video, which would have been a more burdensome obligation for the applicant.

In another case, a judgment by the Supreme Court's Senate (Civil Case Department) reversed a judgment by the Riga District Court in which the latter court ruled that the defendant must ensure that the allegedly defaming content was removed from the Internet (and to futher ensure that it was no longer searchable). The defaming content was a literary work depicting actual persons by their full names in a way that would allegedly interfere with their right to private life.[77] The Senate did not agree with the district court that this content was defaming within the meaning of the law, while not questioning the obligation to remove this content from the Internet if it had been found to be unlawful. However, it should be pointed out that most similar rulings do not impose an obligation to remove the defaming or untrue content from the Internet but rather to withdraw the content (i.e. publish the statement admitting the content was untrue) without specifying that it also has to be removed.

3. Procedural Aspects

There are, generally, three types of public bodies in Latvia that have a competence to decide on the blocking or taking down of Internet content: administrative bodies (Lotteries and Gambling Supervision Inspection and Data State Inspectorate), State police and judiciary bodies (Administrative courts and courts of general competence). The scope of competence and the procedural steps up to the actual restriction varies, depending on the body which is involved.

Only **the Lotteries and Gambling Supervision Inspection** has an express provision in law authorizing it to request the blocking and prescribing the steps that need to be followed. The governmental decree[78] specifies that the Lotteries and Gambling Supervision Inspection prepares a decision to restrict access to a website of the organizer of the interactive gambling which is not licensed in Latvia. The inquiry (filed electronically on a specific form provided for in the decree) is to be sent at least once in three months to the holder of the top level domain name .lv and the electronic communications merchant. [79] The merchant and the holder are required to implement the decision within five working days. The restriction is to be kept in effect until the day when the merchant receives the decision by the Inspection to lift the restriction (blocking) and it must then restore access within five working days. The Law and the Decree do not specify the procedure for the un-

---

76 Judgment of 2 June 2014 in Case Nr. A420502213.

77 Judgment of 12 September 2012 mentioning the judgment by the District court of 19 March 2009 (the latter judgment not available online).

78 "Rules applicable to the Lotteries and Gambling Supervision Inspection preparation and sending of the decision on the restriction of access to the interactive gambling organizers' Internet home pages which are not licensed in Latvia", Governmental decree (Cabinet of Ministers) nr 291 adopted on the 9 June 2014, in effect as of 1 August 2014 (this author's translation).

79 Section 19(1)(22) of the Electronic Communications Law.

blocking of the site in cases where the court rules to annul the decision of the Inspection. General provisions of the Administrative Procedure Law will apply in such cases. Lastly, the Electronic Communications Law provides that the "electronic communications merchant" is not liable for damages caused by the decision to restrict access of the Lotteries and Gambling Supervision Inspection to third parties.[80]

The Data State Inspectorate is competent to adopt a decision to block (remove) protected personal data. The law provides the Inspectorate with competence to enter non-residential premises and to obtain help from law enforcement agencies. In practice, the Inspectorate would send a request to the person or entity which has published the protected data. The law does not contain provisions regulating the notification of a person who actually published the protected data, if the addressee of the decision is a different person or entity (for example, a portal owner).

In both cases described above, the law expressly provides for the possibility of a review of decision by administrative courts (independent judicial bodies), subject to general administrative procedures.

In cases concerning Internet content that allegedly amounts to defamation or copyright infringement, **civil courts** will be competent to adopt a decision to remove (have removed) the Internet content in question. There are no special provisions governing the blocking or removal of such information on the Internet, and general civil procedural rules will apply. In cases involving media governed by the Electronic Media Law, the affected individual may turn to the court to have the untrue information removed. In such a case, it is necessary to obtain a valid judgment binding on the publisher (website owner) to remove the information, which can either be executed voluntarily or through a bailiff, subject to generally applicable procedure.

The **State police** will adopt a decision to block or remove Internet content in cases involving allegedly criminal infringements. The decision can be taken in the shape of a seizure or security measure (prohibition of employment, as the practice shows), which means that it has to be preceded by a decision to institute a criminal investigation. In cases of seizure, a copy of the decision on seizure will be issued to the person at whose site the seizure is taking place.[81]

In cases of prohibition of employment, a copy of the decision is to be sent to employer or "another relevant authority".[82] The addressee of such a measure may appeal the measure one time to the investigating judge, whose decision on appeal is final.[83]

4. General Monitoring of Internet

In principle, no state entity exists in Latvia that would have an obligation to pro-actively monitor Internet content as a whole. Monitoring of Internet content is generally performed by users of Internet themselves, who may report about supposedly illegal content to some institutions mentioned below or to the ISP.

With respect to preventing the distribution in Latvia of material relates to sexual abuse of children and other criminal pornography, the **Latvian Internet Association** runs the Net-Safe Latvia. Net-Safe

---

80 Section 19(3) of the Electronic Communications Law.

81 Section 188(1) of the Criminal Procedure Law.

82 Section 254(2) of the Criminal Procedure Law. It is not clear from the practice how exactly this notification is made in case of blocking a website (only one case reported where this measure was used).

83 Section 262.

(Safer Internet Center)[84] has its own website where any Internet user can notify an infringement discovered on-line by sending notification via the Center's website www.drossinternets.lv. Processing of such notifications is conducted by Net-Safe in cooperation with the police. Police may subsequently issue permission to the Center to make contact with the Electronic Merchants which, in turn, perform the take-down of the illegal content from the Internet. However, nothing in the Latvian law prevents users from contacting the police directly in the event that they discover content that they believe is illegal on the Internet.

Cert.lv is an institution for the prevention of information technologies security incidents and is run by the Agency of the University of Latvia "Mathematics and Informatics Institute of the University of Latvia». Cert.lv ensures IT security in Latvia according to the Law on Information Technologies' Security. Cert.lv receives and processes information about security incidents of different priorities but this does not appear to include the content of Internet as such. However, cert.lv also cooperates with Net-Safe and is, in particular, party to the voluntary memorandum described earlier.

Data State Inspectorate has a task of supervising the protection of the personal data generally, including such data on the Internet.

The State police does not monitor Internet but receives notifications about allegedly illegal content from Internet users, private persons or public institutions.[85]

Law on Information Society Services[86] envisages that information societies' supply of services is supervised by the Data State Inspectorate and the Consumer Protection Agency (and, as the case may be, other institutions) which may monitor the activities of such societies and require them to stop activities that amount to infringements.[87]

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

Generally, freedom of expression as well as limitations on the freedom of speech, e.g. prohibition of defamation, hate-speech, etc. apply to the Internet in the same scope as they apply to other means of publishing or expression. This has been firmly established in Latvian court practice.[88] In addition, Article 100 of the Constitution (Satversme) prohibits censorship. It must be noted from the outset that Latvian practice in this field is mainly to refrain from blocking (especially wholesale blocking) and restricting Internet content, and cases where such was undertaken (other than in cases of illegal pornography) are very few.

In Latvia, the only law which expressly and specifically provides for blocking the content of the Internet is the law regulating **blocking of unlicensed on-line gambling sites**. The legal provision on blocking in this context is laid down in the Electronic Communications Law, whereas the requirement to obtain a license in Latvia is laid down in a separate statute dealing specifically with gambling. The rule on blocking of unlicensed gambling sites is sufficiently clear and precise, as well as foreseeable

---

84 http://www.lia.lv (07.08.2015).

85 For example, Ombudsman of Latvia has recently sent a letter to the Chief of the State Police informing about a video on youtube.com containing child sexual abuse. The Ombudsman itself does not have a competence to generally monitor internet or to have the contents blocked or removed.

86 Adopted on 4 November 2004, in effect as of 1 December 2004.

87 Section 12.

88 E.g., the Senate of the Supreme Court of Latvia ruled on 17 October 2012 in Case SKC-637/2012 that the Law on Mass Media applies also to such media that operate in the electronic environment, such as Internet portals.

because the affected individual or company knows the conditions to be met for being able to operate the on-line gambling site. No wholesale blocking as such is permitted in the Law.

The provision envisaging blocking of unlicensed gambling sites is relatively new, and the compatibility of this new provision with human rights, i.e. the freedom of expression, may be questioned. However, it is unlikely to affect any rights guaranteed by the European Convention on Human Rights. It is also possible to obtain a license, according to the conditions specified by law, to avoid having the site blocked. In any case, the affected individual or company (owner of the gambling site) has access to the administrative and judicial review. There has so far been only one case addressing the question of blocking of such a site where the legality of blocking was examined in light of the national law definition of "gambling", and not from a human rights perspective.

It can be concluded that in respect of blocking of unlicensed on-line gambling sites the Latvian law and practice does not interfere with the rights protected by the ECHR.

The provisions requiring the **removal of sensitive personal data** also provide for a possibility to request if not blocking of a site where the data appeared, removal of the unlawful Internet content. The definition of protected data in the Data Protection Law is formulated relatively generally and has to be interpreted in specific cases. Thus, it has been interpreted to include a video of policemen posted on the YouTube, faces and voices of individual policemen being considered as protected by the law.[89] The law is not as such unnecessary or disproportional, although it may be questioned whether the interpretation given to the protected data was too broad, at the cost of the freedom of expression.

This law does not provide for a legal basis of blocking the Internet or a specific site as a whole, so YouTube was not blocked (in line with general practice in Latvia). However, as this case illustrates, the owner of the video may be requested to remove the video from Internet. The court examined the question of the necessity and proportionality of this decision. The court noted that the decision was not disproportionate, as the applicant was not asked to destroy the video, only to remove it from the Internet. However, a **less restrictive measure** would be to request the owner of the video to manipulate the video to ensure that faces and voices on the video are not possible to identify. Then, the video would still translate the author's critical message (allegedly poor work of the police) and his freedom of expression would not be compromised. In the absence of other similar cases, it is difficult to judge whether there is some systematic inconsistency between Latvian national court practice and the case law of the ECtHR.

The law meets the requirement for access to judicial review, and the owner of the video availed himself of this possibility, although he ultimately chose not to appeal the first instance's ruling.

Although there are few court cases addressing the blocking or restriction of the Internet, the court system is sufficiently open for individuals in cases where the restrictions are related to cases of administrative character.

It can be concluded that in respect of removal of personal data from Internet, the law provides for necessary safeguards which have been implemented in practice but substantive provisions of the law still may be interpreted by the courts in a way which encroaches upon the requirement of proportionality.

As the **criminal procedural rules** have also been used in practice as a legal basis to restrict or block the Internet sites (albeit in very few cases), it is necessary to determine whether such rules are in line

[89] Judgment of 2 June 2014 in Case Nr. A420502213.

with the requirements of the ECtHR. There is no case law in Latvia directly addressing this question. In light of the ECtHR, the following should be noted:

The provisions of the Criminal Procedure Law are generally formulated and do not specifically address cases where the blocking, filtering or taking down of content on the Internet may be necessary. The **Criminal Law** also only formulates the infringements which are prohibited and amount to criminal offences, triggering application of the procedural measures laid down in the Criminal Procedure Law. However, both laws are silent on situations when the public authority (police) considers that the content is unlawful and needs to be removed from the site, or the site needs to be blocked before there has been rendered a judgment on the merits.

In cases, where the decision to remove or block the Internet site is taken before a judgment on the merits has been adopted (as is the case in the practice described earlier), the decision would be of preventive character, i.e. before the ruling on the merits has been adopted and may for this reason constitute a **prior restraint**, which may interfere, *inter alia*, with a right to receive or distribute information.[90]

According to the case law of the ECtHR, the interference with the Internet access must be prescribed by law, pursue a legitimate aim laid down in an ECHR provision (e.g. Article 10.2) and be necessary in a democratic society to achieve such an aim.[91] The **Criminal Procedure Law of Latvia does not contain provisions** expressly envisaging the blocking or restriction of illegal Internet content. The legal basis for such measures could be found in the provisions on seizure or in the prohibition from employment. These are pre-trial security measures which only apply to the suspect or the accused if there are grounds to believe that the relevant person will continue criminal activities, or hinder pre-trial criminal proceedings or court or avoid such proceedings and court.[92]

Pre-trial security measures are applied only to the suspect (for example, owner of a specific site, a group on a portal, a particular material posted and the like), and not an unlimited number of people. To the extent they only target the specific contents, they may meet the requirement not to block the Internet access on a wholesale basis.[93] However, these provisions still do not appear to be well-suited to address all possible situations arising due to the need to block or remove the Internet content. Thus, seizure procedures may be well suited to cases when a server can be seized, but not so well to cases when the contents is blocked without server being seized, for example, foreign-based contents. Also, it is not clear what would happen if the police consider it necessary to seize the whole domain, thereby affecting owners of other sites, email addresses, etc. incidentally? This may constitute a disproportionate restriction not permitted by ECHR.

Further, **prohibition from certain employment activities is unlikely to be an appropriate ground** for blocking a website or portal as a whole if the allegedly illegal content is posted on a specific site, in a forum or on a blog. In such a case, the restriction would exceed what is allowed in light of necessity. In any case, prohibition from certain employment the way it is formulated in the law does not seem to be appropriate to provide a legal basis for blocking or restricting Internet content, as it would not meet the criteria for the sufficient clarity and foreseeability, and would not provide for a protection against arbitrary interference by the public authority.[94]

---

90 *Ahmet Yildrim v. Turkey*, 18 December 2012, para 48, *Times Newspapers Ltd v. The United Kingdom*, 10 March 2009, para 27.

91 *Ahmet Yildrim v. Turkey*, para 56.

92 Section 241 of the Criminal Procedure Law.

93 *Ahmet Yildirim v. Turkey*.

94 *Ahmet Yildirim v. Turkey*, para 59.

It should, however, be noted that Section 12(1) of the Criminal Procedure Law generally requires that criminal proceedings are performed in conformity with internationally recognised civil rights and without allowing for the imposition of unjustified criminal procedural duties or excessive intervention in the life of a person.

The **Law on Operational Activities** contains even more general and vaguely formulated provisions, which do not address the competence to block or remove directly. In this case, the blocking or removal would clearly constitute a prior restraint that would not comply with the criteria of clarity and foreseeability of the law.

Secondly, there is a **limited possibility for judicial review of pre-trial security** measures laid down in the Criminal Procedure Law. It can be pointed out in this respect that an appeal can be only made by a person with the status of the suspect or the accused (or a representative of this person) so that persons who are not the addressees of the decision may not avail themselves of this appeal procedure. In addition, it is necessary to justify that the appealed security measure may not be fulfilled by the suspect or accused.[95] It can be concluded that these provisions do not ensure effective judicial review to prevent abuse of power, as required by the ECHR.[96]

It can be **concluded** that the security measures described above will not meet the ECtHR requirements on the quality of the law, because the scope of discretion enjoyed by the authority is very unclear and access to safeguards such as possibility of review is limited. [97]

As to the **self-regulatory frameworks** in Latvia, these are related to combatting distribution of illegal and punishable (criminal or administrative) materials, mainly with a view of child protection. The safeguards would be found in the criminal procedural provisions examined above.

10 August 2015

Alla Pozdnakova

[95] Section 262(2).

[96] Ahmet Yildirim, para 64, Association Ekin v France, para 58, Editorial Board of Pravoye Delo v Ukraine, para 55.

[97] Ahmet Yildirim, para 59, The Sunday Times, Maestri v Italy.