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 193-217

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.

ESTONIA

1. Legal Sources

Estonian legislators have been very restrained in imposing limitations on freedom of expression on the internet or on access to the internet in general. Estonia does not have any separate statute devoted specifically to the internet, nor are there any specific provisions under Estonian law concerning the blocking, filtering, or removal of illegal internet content. The blocking of domain names, as a measure available for use in cases of illegal internet content, is expressly permitted only in connection with cases of illegal remote gambling, as set forth in the 2008 Gambling Act (GA § §56, para. 2).[1]

More generally, it is the Information Society Services Act (ISSA)[2] that governs the blocking and removal of illegal internet content. Under that act, supervisory authorities may request that the concerned internet service providers (ISPs) take the appropriate actions. The administrative procedures to be followed when taking such measures are contained in the Administrative Procedure Act, which also governs ISP supervision.

Estonia has ratified the following relevant conventions:

- Council of Europe Convention on Cybercrime, signed 23 November 2001, ratified 12 May 2003; Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, signed 28 January 2003, not ratified;
- Council of Europe Convention on the Prevention of Terrorism, signed 7 September 2005, ratified 15 May 2009;
- United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965, ratified 21 October 1991;
- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of 25 October 2007, signed 17 September 2008;
- United Nations Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, of 25 May 2000, ratified 12 February 2004.

In addition to the ISSA, a number of other statutes also contain individual provisions defining the substantive conditions for imposing legal restrictions on freedom of expression, and establishing the precise procedures to be followed when making decisions (issuing administrative requests or orders) on the blocking, filtering, or removal of illegal internet content. These include the Security Authorities Act, the State Secrets and Classified Information of Foreign States Act, the Estonian Defence League Act, the State of Emergency Act, the Money Laundering and Terrorist Financing Prevention Act, the National Defence Act, the Penal Code, the Code of Enforcement Procedure, the Police and Border Guard Act, the Child Protection Act, the Act to Regulate Dissemination of Works which Contain Pornography or Promote Violence or Cruelty, the Emergency Act, the Gambling Act, the Personal Data Protection Act, the Public Information Act, the Electronic Communication Act, the Law of Obligations Act, the Copyright Act, the Trade Marks Act, the Code of Civil Procedure, the Conciliation Act, the Administrative Procedure Act, and the Criminal Records Database Act. Depending on the nature of any individual case, it is quite possible, or even likely, that multiple laws,

[1] Gambling Act, adopted 15 October 2008, entered into force 1 January 2009, English translation available at https://www.riigiteataja.ee/en/eli/511052015004/consolide.

[2] Information Society Services Act, adopted 14 April 2004, entered into force 1 May 2004, English translation available at https://www.riigiteataja.ee/en/eli/513012015001/consolide.

as well as the relevant case law, soft law instruments, and arguments from the legal literature will come into play.

The main safeguards against arbitrary blocking and filtering are the Constitutional provisions guaranteeing the basic rights and freedoms of individuals. Article 11 of the Constitution provides that rights and freedoms may be circumscribed only to the extent permitted by the Constitution. Such curtailment of rights must be in keeping with the demands of a democratic society and must not distort the fundamental nature of the rights and freedoms being restricted. Any individual whose rights or freedoms have been infringed the by the blocking or filtering of internet content, is entitled to apply for relief to the courts. The Constitution (§ 15) vests the courts with the authority to declare unconstitutional any law, other legislative instrument, administrative decision, or official measure that is found to be relevant to the matter at hand. Under § 26 of the Constitution, interference with any individual's private or family life is permitted – in the cases contemplated by the law and in keeping with the prescribed procedures – in order to protect public health, public morality, public order or the rights and freedoms of others, to prevent a criminal offence, or to apprehend an offender. All persons are entitled to free access to information disseminated for public use. In § 44, the Constitution stipulates that there is to be no censorship in Estonia. Every person has the right to freely disseminate ideas, opinions, beliefs and other information by word, print, picture or other means. This right may be circumscribed only by legislative act, in order to protect public order, public morality, and the rights and freedoms, health, honour, and good name of others (Constitution § 45).

Estonia follows EU court practice, and EU law is transposed into Estonian law as required. The following Directives have been transposed in Estonian legislation:

- Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA;
- Directive 2000/31/EC of the European Parliament and the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal market; and
- Directive 98/48/EC of the European Parliament and the Council of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations

2. Legal Framework

Measures such as the filtering, blocking, or take-down of illegal internet content may be imposed in the situations and under the conditions prescribed by law, at the order of supervisory authorities or the courts. They may be imposed as measures contemplated under the rules for self-regulation of ISPs, internet platforms, etc.

The regime for the blocking, filtering, or take-down of internet content in Estonia relies on the model calling for a centralized, *ex ante* process for indicating illegal content (by supervisory authorities or other parties), with enforcement carried out by the ISPs. The grounds that may be invoked for exercising the power to restrict illegal internet content are set forth in special laws, which also list the supervisory authorities that have been vested with that power. The following section outlines the main grounds that may be invoked by public supervisory authorities in decisions on the restriction of illegal internet content and the procedures foreseen for the enforcement of their official decisions, administrative requests, and orders, as set forth in the respective legal sources.

National Security, territorial integrity and public safety

- - The Constitution of the Republic of Estonia (Constitution)[3] stipulates in § 129 that a state of emergency may declared, where provided by law, in the face of a threat to the constitutional order. The relevant legal provision is contained in § 3 of the State of Emergency Act (SEA)[4], which sets out the circumstances capable of giving rise to such a threat: an attempt to overthrow the constitutional order of Estonia by violence; terrorist activity; collective coercion involving violence; extensive conflict between groups of persons involving violence, forceful isolation of an area of the Republic of Estonia; and prolonged mass disorder involving violence. Under § 130 of the Constitution, in a state of emergency, the rights and liberties of persons may be restricted in the interest of national security and public order. The restriction of rights and liberties during a state of emergency is held to be warranted only for the purpose of responding to a threat to the constitutional order.
- The Estonian Security Authorities Act (SAA)[5] defines the functions and powers of security authorities for ensuring national security and the constitutional order. It also establishes the procedure for oversight over the activities of the security authorities. There are no provisions empowering the security authorities to block, filter, or remove internet content. Moreover, the authorities are enjoined to use only such measures as are necessary for performing their duties, and which impinge upon the fundamental rights of individuals to the smallest degree possible (SAA, § 3 para. 2).
- The Police and Border Guard Act (PBGA)[6] governs the functions, powers and organisation of the police force. With regard to the duties and conduct of the police in criminal proceedings, it refers to the Code of Criminal Procedure (CCrP)[7] and the Code of Misdemeanour Procedure (CMP);[8] with regard to the protection of public order, it refers to the Law Enforcement Act (LEA)[9] (PBGA § 1). It does not, however, make provision for any police measures for the blocking or taking down of internet content other than in the context of criminal proceedings.[10]
- The State of Emergency Act (SEA)[11] authorises restriction of the rights and liberties of individuals where a state of emergency has been declared, in the interest of national security and preserving public order (SEA § 17, para. 1 [7] and [8]). The Money Laundering and Terrorist Financing Prevention Act[12] establishes the authority of the Data Protection Inspectorate to act to prevent the use of the financial system and economic territory of Estonia for purposes of money laundering and terrorist financing.

---

3 The Constitution of the Republic of Estonia, adopted 28 June 1992, entered into force 3 July 1992; English translation available at https://www.riigiteataja.ee/en/eli/521052015001/consolide.

4 State of Emergency Act, adopted 10 January 1996, entered into force 16 February 1996; English translation available at https://www.riigiteataja.ee/en/eli/ee/517122014004/consolide/current.

5 Estonian Security Authorities Act, adopted 20 December 2000, entered into force 1 March 2001, English translation available at https://www.riigiteataja.ee/en/eli/507042015002/consolide.

6 Police and Border Guard Act, adopted 06 May 2009, entered into force 1 January 2010, English translation available at https://www.riigiteataja.ee/en/eli/515042015002/consolide.

7 Code of Criminal Procedure, adopted 12 February 2002, entered into force 1 July 2004, English translation available at https://www.riigiteataja.ee/en/eli/501042015002/consolide.

8 Code of Misdemeanour Procedure (CMP), adopted 22 May 2002, entered into force 1 September 2002, English translation available at https://www.riigiteataja.ee/en/eli/503082015005/consolide.

9 Law Enforcement Act, adopted 23 February 2011, entered into force 1 July 2014, English translation available at https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/516062015011/consolide.

10 Judgment of the Estonian Supreme Court in criminal case no. 3-1-1-57-32, pp. 15-16.

11 State of Emergency Act, adopted 10 January 1996, entered into force 16 February 1996, English translation available at https://www.riigiteataja.ee/en/eli/ee/517122014004/consolide/current.

12 Money Laundering and Terrorist Financing Prevention Act (MLTFPA), adopted 19 December 2007, entered into force 28 January 2008, English translation available at https://www.riigiteataja.ee/en/eli/502042015014/consolide.

- One of the most important areas of cybersecurity is regulated in the State Secrets and Classified Information of Foreign States Act (State Secret Act),[13] which governs, among other things, the government's cybersecurity measures and the structure of the public supervisory authorities. In this area, the Estonian government works in cooperation with private and non-governmental entities. A special section has been established within the Estonian Defence League[14] for preventing and deflecting cyberattacks, in collaboration with the cyber security laboratory of the Estonian National Army.[15]
- The Penal Code (PC) [16] designates certain acts of relevance in this context as punishable offences. These include: offences against humanity and international security (PC, Part 2, chapter 8, division 2), including offences against peace (PC, Part 2, chapter 8, division 3); offences against political and civil rights (PC, Part 2, chapter 10); public incitement for the commission to acts of terrorism (PC § 237^2); incitement to participation in mass disorders (PC § 238), disclosure of state secrets and classified information of foreign states (PC §§ 241 and 242), communication of internal information, (PC § 243).

Prevention of civil disorder or criminal activity

While the Penal Code renders punishable a number of criminal offences potentially related to illegal internet content, where such content incites or encourages civil disorder or crime (see previous section), it does not contain any rules on measures for the preventive filtering or blocking of internet content. Such measures are covered by the **Law Enforcement Act** (LEA), which defines law enforcement as "the prevention of a threat endangering public order (hereinafter *threat*), ascertainment of a threat in the case of a suspicion of a threat, countering of a threat and elimination of a breach of public order (hereinafter *disturbance*)." LEA § 6, para. 3 stipulates as follows: "The police shall apply urgent measures for countering an immediate threat or eliminating a disturbance if this does not constitute an excessive obstruction of the performance of the functions of the police."

The protection of health or morals

Emergency Act (EA)[17] § 16 can serve as the statutory basis for blocking internet content in cases where the conditions for the use of measures restricting the fundamental rights of persons are satisfied. This may be the case in an emergency situation, which is defined in EA § 2, para. 1, as "an event or a chain of events which endangers the life or health of many people or causes major proprietary damage or major environmental damage or severe and extensive disruptions in the continuous operation of vital services and resolving of which requires the prompt coordinated activities of several authorities or persons involved by them".

The Penal Code also includes certain offences against minors in which internet content may play a role: influencing persons under the age of 18 to commence or continue in the commission of a crime, to engage in begging, to engage in prostitution or "working under unusual conditions", or to appear as a model or actor in pornographic or erotic performances, where such activity dose not constitute a misdemeanour as defined in PC § 133 (PC § 175 [1]); the illegal use of the identity (including pictures)

---

13 State Secrets and Classified Information of Foreign States Act, adopted 25 January 2007, entered into force 1 January 2016, available in Estonian at https://www.riigiteataja.ee/akt/112032015046.

14 Estonian Defence League Act, adopted 28 March 2012, entered into force 1 April 2013, English translation available at https://www.riigiteataja.ee/en/eli/510032015001/consolide.

15 See also the National Defence Act (in Estonian:e riigikaitseseadus), adopted 11 February 2015, entered into force 1 January 2016, English translation available at https://www.riigiteataja.ee/akt/112032015001.

16 Penal Code, adopted 6 June 2001, entered into force 1 September 2002, English translation available at https://www.riigiteataja.ee/en/eli/ee/519032015003/consolide/current.

17 Emergency Act, adopted 15 June 2009, English translation available at https://www.riigiteataja.ee/en/eli/504092015012/consolide.

of another individual (§ 157[2] of the PC); human trafficking with the intent of abusing minors (PC § 175); the production, acquisition, or any manner of distribution of pictures, films, writings or other media depicting the minors under the age of 14 in erotic or pornographic situations, or of minors under the age of 18 in pornographic situations (PC § 178); proposing or consenting to meet a minor for sexual purposes (PC § 178[1]); sexual enticement of children (minors under 14 years of age) including by the use of pornographic material (§ 179 of the PC); extortion, including by means of erotic or pornographic material in which the victim appears (PC § 214).

The **Act to Regulate Dissemination of Works, which Contain Pornography or Promote Violence or Cruelty**[18] prohibits the dissemination and exhibition to minors of works that contain pornography or promote violence or cruelty (§ 1, para. 1).

The **Republic of Estonia Child Protection Act**[19] prohibits the manufacture or showing of "printed matter, films, audio and video recordings and objects which promote cruelty and violence or cruelty, intended for children" (§ 48), and the production or distribution of obscene or pornographic material for, or to, children, or with their participation (§ 50).

The **Advertising Act (AA)**[20] provides that advertising may not "be contrary to good morals and customs", "incite to act unlawfully or violate prevailing standards of decency, justify offences or degrade lawful behaviour", "incite to activities harmful to human health or the environment", or "exhibit technology and equipment in a manner which may contribute to the feeling of safety not corresponding to the reality or cause dangerous behaviour". Specifically prohibited, for example, are the advertising of works that contain pornography or promote violence or cruelty (AA § 24), the "advertising of services offered for satisfaction of sexual desire", including prostitution services and the procuring of such services. (AA § 25).

The **Gambling Act (GA)**[21] stipulates that "the provider of data storing service shall eliminate the information used for the provision of illegal remote gambling which is stored by a user of the data storing service, or prevent access of such information on the basis of a precept of the Tax and Customs Board by the due date set out in such precept" (GA § 56, para. 1). Further, "the provider of publicly available electronic communication service providing internet access shall, on the basis of a precept of the Tax and Customs Board and by the due date set out in such precept, block the domain name of illegal remote gambling specified in the precept in the domain name servers belonging to such service provider" (§ 56 para. 2 of the GA). A statutory basis for blocking the domain name of an illegal remote gambling platform is also provided by the Gambling Act, in setting out the mandatory conditions for the licensing of gambling operators (GA, chapter 2).

Protection of personal data

According to the **Public Information Act** (PIA),[22] access to information intended for public use is "based on the principles of a democratic and social rule of law and an open society" (PIA § 1). In that

---

18 Act to Regulate Dissemination of Works which Contain Pornography or Promote Violence or Cruelty, adopted 16 December 1997, entered into force 1 May 1998, English translation available at https://www.riigiteataja.ee/en/eli/520012015009/consolide.

19 Republic of Estonia Child Protection Act, adopted 8 June 1992, entered into force 1 January 1993, English translation available at https://www.riigiteataja.ee/en/eli/531102014002/consolide.

20 Advertising Act, adopted 12 March 2008, entered into force 1 November 2011, English translation available at https://www.riigiteataja.ee/en/eli/512052015001/consolide.

21 Gambling Act, adopted 15 October 2008, entered into force 1 January 2009, English translation available at https://www.riigiteataja.ee/en/eli/511052015004/consolide.

22 Public Information Act, adopted 15 November 2000, entered into force 1 January 2001, English translation available at https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/522122014002/consolide.

vein, § 33 of the PIA provides as follows: "Every person shall be afforded the opportunity to have free access to public information through the internet in public libraries, pursuant to the procedure provided for in the Public Libraries Act". One stated purpose of the law is "to create opportunities for the public to monitor the performance of public duties" (PIA § 1).

The Personal Data Protection Act (PDPA)[23] establishes the statutory regime for the processing of personal data, including implicitly the disclosure of such data on the internet (PDPA § 5). Unless otherwise provided by law, the processing of personal data is permitted only with the consent of the data subject (PDPA § 12 and § 11, para. 8)[24]. An exception is made for the processing and disclosing personal data in the media "for journalistic purposes", where there is "a predominant public interest" in such disclosure, provided that it is consistent with journalistic ethics and that it "does not cause excessive damage to the rights of a data subject" (PDPA § 11, para. 2). Personal data may also be processed for the purpose of transmitting it to third parties "for assessing the creditworthiness of persons or other such purpose", subject to certain conditions: first, the third party must have a legitimate interest in processing the personal data; and, second, the person communicating the data must establish that the third party receiving it has a legitimate interest therein, must verify the accuracy of the data to be communicated, and must register the data transmission (PDPA § 11, para. 6). A data subject may demand the cessation of disclosure, provided that it is "technically possible and does not result in disproportionately high costs" (PDPA § 11, para. 4).

The **Code of Criminal Procedure** (CCrP) imposes certain restrictions on the publication of personal data on the internet. Under CCrP § 408[1], para. 1, court judgments and rulings that have entered into force must be published online, exception being made for pre-trial rulings in criminal cases, where the proceedings in question have not been finally concluded. Published decisions include disclosure of the name and the personal identification number or, in the absence of an identification number, the date of birth of the defendant (CCrP § 408[1], para. 2). Information concerning convicted defendants and their sentences is maintained in the Criminal Records Database, within the government information system. Under § 7 of the Criminal Records Database Act (CRDA),[25] data entered into the database are considered as public information, except where otherwise provided by law.

Protection of the reputation of others

Protection of the reputation or rights of others – through anti-defamation rules, invasion of privacy rules, and intellectual property rights) is assured primarily by norms of private law. Defamation is not considered to be a criminal offence, meaning that only civil law remedies are available. Infringement of the personality rights of third parties, including the causing of harm to another's reputation, is dealt with in § 1046 of the Law of Obligations Act (LOA). Para. 1 of that article provides that "the defamation of a person, inter alia by passing undue value judgment, by the unjustified use of the name or image of the person, or by breaching the inviolability of the private life or another

---

23 Personal Data Protection Act, adopted 15 February 2007, entered into force 1 January 2008, English translation available at https://www.riigiteataja.ee/en/eli/ee/529012015008/consolide/current.

24 § 14 of the PDPA provides a limited list of exceptions to the consent rule if the personal data are to be processed: 1) on the basis of law; 2) for performance of a task prescribed by an international agreement or directly applicable legislation of the Council of the European Union or the European Commission; 3) in individual cases for the protection of the life, health or freedom of the data subject or other person if obtaining the consent of the data subject is impossible; 4) for performance of a contract entered into with the data subject or for ensuring the performance of such contract unless the data to be processed are sensitive personal data. These rules are derived from article 7 of Directive 95/46/EC.

25 See the Criminal Records Database Act, adopted 17 February 2011, entered into force 1 January 2012, English translation available at https://www.riigiteataja.ee/en/eli/520022015001/consolide.

personality right of the person is unlawful unless otherwise provided by law". Also qualified as unlawful is "the violation of personality rights or interference with the economic or professional activities of a person by way of disclosure of incorrect information or by the incomplete or misleading disclosure of factual information concerning the person or the activities of the person (LOA § 1047, para. 1). Similarly, the disclosure of defamatory information or of economically damaging facts is declared unlawful, "unless the person who discloses such facts proves that the facts are true." An exception to the prohibition on such disclosure is made where the person who discloses the information or to whom it is disclosed has "a legitimate interest in the disclosure" and subject to the condition that "the information was checked with a thoroughness which corresponds to the gravity of the potential violation" (LOA § 1047). Here, the blocking of access to the information could potentially be one of the measures ordered by a court. Invasion of privacy, as a form of illegal behaviour, is addressed in various specific laws.

The Money Laundering and Terrorist Financing Protection Act (MLTFPA) imposes restrictions on access to information transmitted to the Financial Intelligence Unit (MLTFPA § 43). The Financial Intelligence Unit is empowered to establish restrictions on the use of the data transmitted of its own accord to other government authorities.
The Code of Misdemeanour Procedure (CMP) provides that "information concerning pre-trial proceedings may be disclosed before making of a decision in the interests of the misdemeanour proceeding…only if disproportionate damage is not caused thereby to the misdemeanour proceeding, interests of the state or business secrets or, in particular in the case of disclosure of sensitive personal data, to the rights of data subjects or third persons" (CMP § 62).

Information received in confidence
There are no statutory rules devoted specifically to the blocking or filtering internet content for the purpose of preventing the disclosure of information received in confidence. The Media Services Act (MSA) provides, in general, that "a person who is processing information for journalistic purposes shall have the right not to disclose the information that would enable identification of the source of information" without the consent of the source. The information in question may be disclosed only "pursuant to the conditions and in the procedure provided for in the Code of Criminal Procedure". These restrictions apply also to any person "who is professionally exposed to information that enables identification of the source of information" (MSA § 15).

Information received in confidence is protected in addition pursuant to clause 31 of subsection 1 of § 72 of the Code of Criminal Procedure. The latter provides that journalists have the right to refuse to give testimony as witnesses concerning the circumstances which have become known to them in their professional or other activities. More specifically, such right extends to persons processing information for journalistic purposes regarding information which enables identification of the person who provided the information, except in the case when gathering evidence through other procedural measures is precluded or especially complicated. In addition, such right may only be used if the object of the criminal proceeding is a criminal offence for which at least up to eight years' imprisonment is prescribed as punishment, there is predominant public interest for giving testimony and the person is required to give testimony at the request of a prosecutor's office based on a ruling of a preliminary investigation judge or court ruling. Thus, it clearly influences any blocking or filtering of internet content which has been published for journalistic purposes, as such content cannot be removed in the context of criminal proceedings without meeting a strict legal criteria.

Intellectual property rights

Intellectual property rights and related rights, including industrial property rights, are protected under a number of statutes. The Law of Obligations Act (LOA)[26] establishes, as a general principle, the unlawfulness of violating the rights of ownership, possession, or similar rights of third parties (LOA § 1045, para. 1 [5]); the blocking or removal of illegal content protected by copyright may be ordered under LOA § 1055. The Copyright Act (CoA)[27] provides for protection of copyright and related rights (CoA § 1). The Trade Marks Act (TMA)[28] provides protection against the infringement of exclusive rights of use to a trademark (TMA § 14). Limitations on the exclusivity of rights are set forth in TMA § 16.

Under the provisions of § 219 of the Penal Code (PC), the "disclosure of a work or performance of a work, invention, industrial design or layout-design of an integrated circuit of another" in one's own name is a punishable offence. The "unlawful public performance, showing, transmission, re-transmission or making available to the public of works or objects of related rights in professional or economic activities" is punishable under PC § 223. The "advertising of equipment or software enabling illegal access to fee-charging information society services or pay-TV or pay-radio programmes or broadcasts, or services enabling access to such services, programmes and broadcasts" is punishable under PC § 225[1].

3. Procedural Aspects

Extra-judicial procedure and competence of state supervisory authorities

The main legal foundations in place for warranting the removal of illegal internet content in Estonia are the constitutional principles of legitimacy, necessity, and proportionality, which must be respected both in the legislative process and in the practice of the courts. All orders, directives, and rulings concerning restrictions on internet content must have a statutory basis and be issued in accordance with the applicable procedural requirements. The removal of illegal internet content can take place voluntarily, at the request or order of the supervisory authority or another government agency, or in response to a court order. Official acts calling for the removal of internet content may be challenged; final authority in such cases lies with the courts.

Under the Information Society Services Act (ISSA), an internet service provider has a duty to remove or block illegal internet content in the following instances: (1) where the service provider has "actual knowledge" either of the removal or blocking of content at the initial source of the transmission thereof, or of an order by a court, the police or a public supervisory authority requiring suppression of the content (ISSA § 9 [5]); or (2) where the service provider becomes aware of facts or circumstances that render apparent the unlawful nature of an internet activity or of internet content (ISSA § 10, para. 1 [2]). This latter rule is the basis for the most common procedure in use for the blocking or taking down illegal internet content in Estonia, whereby a service provider is officially informed as to the presence of illicit internet content and requested to block or remove it. A review of current practice has confirmed that internet service providers normally take immediate steps to remove content that is obviously illegal (e.g., child pornography) when so requested.

---

26 Law of Obligations Act (LOA), adopted 26 September 2001, entered into force 1 July 2002, English translation available at https://www.riigiteataja.ee/en/eli/ee/516062015006/consolide/current#para1

27 Copyright Act, adopted 11 November 1992, entered into force 12 December 1992, English translation available at https://www.riigiteataja.ee/en/eli/531102014005/consolide.

28 Trade Marks Act, adopted 22 May 2002, entered into force 1 May 2004, English translation available at https://www.riigiteataja.ee/en/eli/518112013005/consolide.

The following supervisory authorities have the authority to assess the legality of internet content and issue directives and/or official decisions in that regard (including imposition of fines) in administrative proceedings:

1) **Data Protection Inspectorate**[29] **–** the most important government agency authorized to issue directives to processors of personal data and to render decisions to enforce compliance with the PDPA (PDPA § 40, para. 1). The Inspectorate has oversight authority for ensuring legal compliance in the processing of information registered in government databases, such as that, for example, of the Financial Intelligence Unit (MLTFPA § 51). Where the processing of an individual's personal data is not permitted under the law, a data subject is entitled to demand of the processor the termination of the processing, termination of disclosure, and the deletion of such data. To do so, the data subject must file a complaint with the processor. Under PDPA § 21 para. 3, it is incumbent upon the processor in such case to comply with the request, provided that there are no legal grounds for refusal of the thereof, and that the request is not unjustified (§ 21 para. 3 of the PDPA).

   Where no other procedure is provided for by law, a data subject may appeal directly to the Data Protection Inspectorate, or to the courts, in cases where the data subject finds that the processing of the data constitutes a violation of his or her personal rights. With regard to the duties of the person responsible for the protection of personal data appointed by a processor of personal data, the PDPA provides as follows: "If a person responsible for the protection of personal data has informed the processor of personal data of a violation discovered upon the processing of personal data and the processor of personal data does not immediately take measures to terminate the violation then the person responsible for the protection of personal data shall immediately inform the Data Protection Inspectorate of the discovered violation" (PDPA § 30, para. 4); and, "If a person responsible for the protection of personal data is in doubt as to which requirements are applicable to the processing of personal data or which security measures must be applied upon processing of personal data then the person must obtain the opinion of the Data Protection Inspectorate in such matter before the processing of personal data is commenced" (PDPA § 30, para. 5). As of 1 January 2015, the Inspectorate is no longer authorised to initiate proceedings under the Code of Misdemeanour Procedure.

2) **The Consumer Protection Board**[30] **-** oversight over compliance with the safeguards established for the protection of consumer rights under the Consumer Rights Act and other laws. The Director General of the Consumer Protection Board, or an official so authorised by the Director General, may order commercial entities to terminate or refrain from activities harmful to the collective interests of consumers (CPA § 41, para. 1). The orders are officially served on the commercial entity – by registered mail or against return receipt – within two working days of the date on which they are issued (CPA § 41, para. 4). The commercial entity may appeal such an order, and must comply with the order throughout the appeal process, until a final ruling has been issued by a court.

3) **Tax and Customs Board –** has the authority, since 1 January 2010, to order providers of publicly available electronic communication services offering internet access to illegal remote gambling platforms to block the domain names of those platforms within the service provider's own domain. It is incumbent upon the service providers to comply with such orders within the deadline designated in the order. (Gambling Act [GA] § 56, para. 2).[31] The Gambling Act is the only statute that expressly imposes an obligation on the provider of data storing service to remove information used for the providing of illegal remote gambling services, or to block access to such

---

29 *Andmekaitse Inspektsiooni põhimäärus ja koosseis* (Statute and Membership of the Data Protection Inspectorate), available at https://www.riigiteataja.ee/akt/105032013005 (8 November 2015).

30 Consumer Protection Board (*Tarbijakaitseamet*), http://www.tarbijakaitseamet.ee/en.

31 Gambling Act, adopted 15 October 2008, entered into force 1 January 2009, English translation available at: https://www.riigiteataja.ee/en/eli/511052015004/consolide.

information, on the basis of an order issued by the Tax and Customs Board (GA § 56, paras. 1 and 2). The Estonian Tax and Customs Board have released a blacklist naming 175 illegal online gambling sites.[32] The list, which is updated regularly, is publicly accessible on the Board's website. All procedural issues relating to the blocking of domain names and the publication of blacklists naming illegal sites, as well as the procedures for challenging decisions of the Board, are governed by the Administrative Procedure Act[33] (APA), Code of Administrative Court Procedure[34] and the State Liability Act.[35] Where a server has been blocked without legal warrant, the owner of the server may submit an application to the administrative court to have the administrative act issued by the Tax and Customs Board vacated. The reversal of an administrative act may also be sought by filing contest in an administrative procedure. An application for damages may be submitted to the administrative authority that caused the damage; where that fails, an action may be brought before an administrative court.

4) **State Agency of Medicines** – authorised to issue orders and impose penalties in connection with the advertising of narcotic drugs and psychotropic substances.
5) **Financial Supervision Authority** - oversight of compliance with legal requirements applicable to the advertising of financial services provided to private customers; authorised to issue orders and impose fines.
6) **Agricultural Board** - oversight of compliance with legal requirements applicable to the advertising of plant protection products (AA § 30, para. 2 [3]); authorised to issue orders and impose fines.
7) **Health Board** - supervisory body, functioning as a law enforcement authority, responsible for the oversight of advertising for medical devices and health services (AA § 30, para. 2 [2]; e.g., banning of advertising for infant formulae); authorised to issue orders, impose fines, in keeping with the procedure prescribed in the Substitutive Enforcement and Penalty Payment Act (AA § 32). Orders are subject to appeal before the administrative courts.

LEA § 6, para. 2 provides as follows: "If ascertainment and countering of a threat or the elimination of a disturbance is not within the competence of any other law enforcement agency, it is within the competence of the police." In cases where urgent measures are required, it is incumbent upon the police to take them ("urgent competence" – observing in all cases the principles applicable to "the performance of state supervision" – and to notify the competent law enforcement agency thereof immediately (LEA §§ 6-9 of the LEA). The **Police and Border Guard Board** has no independent authority to issue decisions concerning illegal internet content. The Board is authorised to apply the official supervision measures and is required to "cooperate with other persons and authorities within its competence to prevent and counter a threat endangering public order and to eliminate disturbances" (Police and Border Guard Act [PBGA § 7^{7}).

Where a party with access to a server on which illegal internet content is available fails to respond to an administrative request or order, a number of options exist. If neither the party with access to the server, nor the party who made the illegal content available removes or blocks access to that content, the official oversight authority may report this to the police. The police may then take the measures provided for by law in order to identify the party who posted the illegal content (conduct

---

32 The list of domain name servers of the illegal online gambling sites is available at http://www.emta.ee/index.php?id=27399&tpl=1049 (8 November 2015).

33 Administrative Procedure Act, adopted 6 June 2001, entered into force 1 January 2002, 58, 354, English translation available at https://www.riigiteataja.ee/en/eli/530102013037/consolide.

34 Code of Administrative Court Procedure, adopted 27 January 2011, entered into force 1 January 2012, English translation available at: https://www.riigiteataja.ee/en/eli/530032015001/consolide.

35 State Liability Act, adopted 2 May 2001, entered into force 1 January 2002, English translation available at https://www.riigiteataja.ee/en/eli/515112013007/consolide.

of an enquiry into an electronic communications undertaking, subject to authorisation by the Prosecutor's Office, PBGA § 7[49]). Once the party in question has been identified, based on information forwarded by other public authorities or by private individuals, the police may implement the measures provided for by law. In practice, the usual measure would be seizure of the server in order to prevent continued access to the illegal content. Before taking such action, the official (police officer) "who is about to apply a state supervision measure" is required under the terms of LEA § 11, para. 2, to "identify himself or herself in a clear manner to a person in respect of whom he or she is planning to apply the measure, present at the person's request a document certifying his or her authority (identification), and provide at the person's request explanations concerning the measure to be applied and circumstances specified in … the Administrative Procedure Act". A written record of the measure applied must be prepared, and the party against whom it was applied must be given a copy thereof, at that party's request, as expeditiously as possible. The police are authorized to conduct physical examinations of movable property, either manually or with aid of technical devices, also without the consent of the possessor, where this is deemed necessary for preventing, ascertaining or countering a threat, or for eliminating a disturbance, subject to compliance with the procedural requirements prescribed by, or on the basis of, the law (LEA § 49). Seizure of a server by the police is authorised under the terms of LEA § 55, para. 1, which governs the authority of the police to seize movable property where necessary "for countering an immediate threat or for eliminating a disturbance" (LEA § 52, para. 1). In such case, the party from whom the property has been seized must receive a copy of the seizure report without delay.

In the event of failure to comply with an administrative order, the supervisory authorities may also impose a **monetary fine,** in accordance with the procedures prescribed in the Substitutive Enforcement and Penalty Payment Act.[36] Under the terms of § 10 of that act, the maximum fine to be imposed must be stated in a separate statute. Where this has not been done, the maximum amount of each fine imposed is fixed at EUR 9600.

Where a party fails to comply with an administrative order within the designated time limit, the enforcement authority is required to file a complaint with an administrative court, in accordance with the procedure prescribed in the Code of Administrative Court Procedure. If the decision to remove illegal internet content was made by the court, the usual enforcement procedure applies. However, the filtering, blocking or removal of internet content is not expressly named among the enforcement instruments contemplated in § 2 of the Code of Enforcement Procedure (CEP).

In addition to bringing action for the removal of comments or other illegal data from the internet (online comment sites, blogs, social media etc.), a person whose rights have been violated, is entitled under § 180 of the Code of Civil Procedure [check reference; does not correspond to English version] to seek the identification of a party's Internet Protocol address. If a processor of personal data fails to comply with an order from the Data Protection Inspectorate, the latter may also "address a superior agency, person or body of the processor of personal data for organisation of supervisory control or commencement of disciplinary proceedings against an official" (PDPA § 40[1]).

Under Estonian law there are also procedures for the **extra-judicial resolution of complaints**. The **Estonian Public Broadcasting Act (PBA)** establishes a procedure for resolving complaints in cases where the content of a programme broadcast by Estonian Public Broadcasting – in Estonian *Eesti Rahvusringhääling*, or the ERR – is not in compliance with the provisions of that act (PBA § 39). The independence of the ERR is guaranteed in § 3 of the PBA: "Public Broadcasting shall be independent in the production and transmission of its programme, programme services and other media services

---

36 Substitutive Enforcement and Penalty Payment Act, adopted 9 May 2001, entered into force 1 January 2002, available at https://www.riigiteataja.ee/en/eli/ee/Riigikogu/act/522012015001/consolide (8 November 2015).

and shall be guided exclusively by the requirements of law." The measures contemplated to ensure the preservation of ERR's independence include self-monitoring mechanisms within the ERR's governance structures. Under § 31 of the PBA, an ethics adviser, to be appointed by the management board with the consent of the ERR Council, is charged with monitoring the conformity of the ERR operations with "the professional ethics and good practices of journalism", and reviewing "objections and challenges submitted against the content of a programme". Under the terms of MSA § 20, para. 1, "each natural or legal person, irrespective of the citizenship or location, whose legal rights, particularly reputation, have been damaged by the incorrect presentation of facts in the television or radio service, shall have the right of reply or to apply for implementation of other equivalent remedies that are in accordance with the legislation". Written notice of the intent to reply must be submitted to the television or radio service provider within 20 days from the date of transmission of the programme in question. The television or radio service provider is required to broadcast the reply, free of charge, in the same programme service within 20 days from the date of receipt of the reasoned request (PBA § 20, para. 2). The request to broadcast a reply may be rejected "if the reply is not justified and the request includes a punishable act, or if satisfaction of the request would lead to civil liability for the television or radio service provider, or if generally accepted moral standards would be neglected by satisfaction of the request" (PBA § 20, para. 3). This rule also applies in cases where the information was delivered in the programmes available over the internet.

Under the terms of § 87 of the Copyright Act, the Ministry of Justice is required to establish a **Copyright Committee.** Among the tasks assigned to the Committee is "to resolve, by way of conciliation of the parties pursuant to the procedure set out in the Conciliation Act,[37] the applications submitted concerning measures applicable to allow the free use of works and objects of related rights in certain cases". Where the parties have entered into negotiations with the assistance of the Committee, it is incumbent upon them to conduct the negotiations in good faith and to do nothing to "prevent or hinder negotiations" without just cause. Through conciliation, the Committee can facilitate the resolution of matters relating to the blocking or take-down of illegal internet content that is protected by intellectual property rights. The Committee does not have the power to impose a solution. However, under the terms of § 14 of the Conciliation Act, a settlement between the parties that is reached in conciliation proceedings conducted by the Committee is deemed to be enforceable by the courts. There are no express rules providing for the blocking or removal of internet content as a means of enforcement. The only remedy available would be the imposition of a fine on the party under obligation to remove the illegal content, in cases where the party fails to perform its obligations under the settlement negotiated by the Committee. There is, to date, no case law in Estonia in which the performance of the decisions of the Committee calling for removal of content protected by intellectual property rights is at issue.

In cases where illegal information is publicly broadcast, there are different procedures for the extra-judiciary resolution of complaints. These procedures are outlined in special statutes. For example, § 39, para. 3 of the PBA provides that every person has the right to reply to statements made in a programme broadcast by Estonian Public Broadcasting (ERR). To do so, a complaint must be submitted to the ERR within thirty days from the date of the broadcast. Upon receipt of such a complaint, it is first reviewed by the executive producer of the programme in question, who then decides on whether the reply is to be aired. Where the executive producer decides not to broadcast the reply, the ethics adviser must be informed of that decision. The ethics adviser is then required to prepare a reasoned opinion on the matter and submit it to the management board for a final decision. The ERR has a time limit of thirty days from the date of receipt of a complaint to resolve the matter, either by broadcasting the reply or by issuing a formal decision not to do so.

---

[37] Conciliation Act, adopted 18 November 2009, entered into force 1 January 2010, available at https://www.riigiteataja.ee/en/eli/530102013028/consolide.

Waiver of ISP liability for caching

In implementation of art. 13 (1) of the EU Directive on Electronic Commerce (Directive 2000/31/EC), and in keeping with the practice of the Court of Justice of the European Union (CJEU), the ISSA (§ 9) provides as follows: "Where a service is provided that consists of the transmission in a public data communication network of information provided by a recipient of the service, the service provider is not liable for the automatic, intermediate and temporary storage of that information, if the method of transmission concerned requires caching due to technical reasons and the caching is performed for the sole purpose of making more efficient the information's onward transmission to other recipients of the service upon their request, on condition that: 1) the provider does not modify the information; 2) the provider complies with conditions on access to the information; 3) the provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used in the industry; 4) the provider does not interfere with the lawful use of technology, widely recognised and used by the industry, to obtain data on the use of the information; 5) the provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court, the police or a state supervisory authority has ordered such removal."

Waiver of ISP liability in connection with hosting services

In implementation of art. 12 of the EU Directive on Electronic Commerce, ISSA § 8, para. 1 provides as follows: "Where a service is provided that consists of the mere transmission in a public data communication network of information provided by a recipient of the service, or the provision of access to a public data communication network, the service provider is not liable for the information transmitted, on condition that the provider: 1) does not initiate the transmission; 2) does not select the receiver of the transmission; 3) does not select or modify the information contained in the transmission." ISSA §8, para. 2, defines "acts of transmission and provision of access" as including "the automatic, intermediate and transient storage" of the information in question. Under the terms of ISSA § 10, the service provider is exempted from liability only on condition that, "1) the provider does not have actual knowledge of the contents of the information and, as regards claims for the compensation of damage, is not aware of facts or circumstances from which the illegal activity or information is apparent; and 2) upon obtaining knowledge or awareness of the facts…acts expeditiously to remove or to disable access to the information.

ISP's obligations towards competent supervisory authorities

Internet service providers have a duty to "promptly inform the competent supervisory authorities of alleged illegal activities undertaken or information provided by recipients of their services…and to communicate to the competent authorities information enabling the identification of recipients of their service with whom they have storage agreements" (ISSA § 11, para. 3). Further, they must "submit information at their disposal concerning the recipients of their information storage services to the Prosecutor's Office and investigative body, on the bases and pursuant to the procedure prescribed in the Code of Criminal Procedure, and to a security authority and a surveillance agency, on the bases and pursuant to the procedure provided by law" (ISSA § 11, para. 4). In cases where the court issues individual written requests for information on recipients of information storage services, it is incumbent upon service providers to provide the information at their disposal within the time limit specified by the court in keeping with the procedures prescribed in the Code of Civil Procedure (ISSA § 11, para.5).

Judicial procedure

Certain supervisory authorities are authorised to bring court action on the behalf of the state where there is a general public interest to be protected. Thus, for example, the Consumer Protection Board is authorised to file suit against a commercial entity on behalf of the Republic of Estonia. Before

bringing such an action, however, the Consumer Protection Board must notify the prospective defendant of its intent to file and allow the commercial entity the opportunity to submit a response (CPA § 41[1], para. 3). conversely, administrative measures taken by public authorities (administrative orders, imposition of conditions, prohibitions, etc.) are not subject to immediate contest before the courts. Contestation of an order does not release the commercial entity from its duty to comply with the order until such time as the appeal process has been completed by a reversal of the order by a court. In effect, therefore, the only independent authorities authorised under Estonian law to make a final and unreviewable decision on the right or obligation to block or take-down illegal internet content are the courts (administrative, criminal or civil).

In cases involving defamation of character, invasion of privacy, or unlawful infringement of other personality rights, the injured party may seek the cessation of, or forbearance from, the injurious conduct. The statutory basis for claims arising out of the continued violation of personality rights is found in § 1055, para. 1 of the LOA. While there is, as yet, no case law on the question, it may be assumed that this same article can also be invoked when seeking the removal or blocking of illegal internet content. Where the party against whom the claim is asserted does not have access to, or control over, the internet portal, site, etc., the claim may be formulated so as to require the defendant to submit a demand to the controllers of the information systems in question.[38] The procedure for seeking the enforcement of court orders is set forth in the Code of Enforcement Procedure.[39]

In criminal cases, the procedure prescribed in the Council of Europe Convention on Cybercrime of 23 November 2001 (ratified by Estonia 12 May 2003) applies. Articles 15, 16 and 19 of the Convention provide the statutory basis for measures to render inaccessible, or to remove, illegal computer data in a computer system accessed by the authorities. In practice, the Estonian Supreme Court has directly applied the Convention and has instructed lower courts to the effect that, where possible, the data in question should be copied from the computer, or deleted, rather than seized together with the computer.[40] There is no statutory basis in Estonian law for blocking internet sites within the framework of an ongoing criminal procedure. Under the terms of CPC § 306, para.1, the adjudicating court is to indicate in its judgment the manner in which to proceed with regard to physical evidence and other evidence appropriated, seized, or confiscated in connection with the criminal proceedings. The court may rule that the confiscated evidence (computer, server) is to be destroyed or that illegal data is to be removed from the server.

A party that has been ordered by a government agency to remove illegal internet content is entitled to file contest to the order with the agency in question. If the contest is dismissed, party may then file an appeal with an administrative court, in keeping with the procedure prescribed in the Code of Administrative Court Procedure (APA § 87). Judgments and orders of the administrative courts that have entered into force are immediately enforceable. A bailiff is required to proceed with enforcement in response to a written request by the claimant, supported by an enforceable instrument (CEP § 23, para. 1), of which the original or a properly notarized copy must be submitted together with the request. Where the enforceable instrument is a court judgment, a copy certified by the court office may be submitted; where it is a decision issued in extra-judicial proceedings, a copy certified by the issuing body may be used (CEP § 24, para 4); certification by electronic means or by digital signature is also acceptable (CEP § 23, para. 6).

---

38 See Judgment of the Estonian Supreme Court from 9 December 2010 in civil case no. 3-2-1-127-10, p. 11.

39 Code of Enforcement Procedure, adopted 20 April 2005, entered into force 1.1.2006, available at https://www.riigiteataja.ee/en/eli/513032015004/consolide (8 November 2015).

40 See the ruling of the Estonian Supreme Court of 20 February 2012 in criminal case no. 3-1-1-1-12, pp. 16 and 17, and judgment of 16 May 2012 in criminal case no. 1-1-1-57-12, p. 16.

Where no time limit for voluntary compliance with the enforceable instrument is designated by law or court judgment, the normal procedure calls for the bailiff to fix a deadline – of no less than ten days and no more that thirty days, unless otherwise provided by law. In the absence of compliance, a fine is imposed. This procedure does not appear to be very well suited to judgments ordering the blocking or removal of internet content. As there is, thus far, no case law in this area, it is difficult to predict how application of this procedure would play out in such cases. In actual practice, internet service providers normally comply immediately with all such administrative requests and orders.

4. General Monitoring of Internet

Internet service providers are not subject to any general duty to monitor internet content. The competent supervisory authorities have a general duty of oversight, but no specific duties with regard to the internet. Nevertheless, they do have at their disposal various technical and legal means for preventing or responding to illegal internet content on social media platforms.

Self-regulation: blogs and social media platforms

There are currently over 70,000 active Estonian-language blogs on the internet, including an increasing number of group, project-related, and corporate blogs. The traditional media frequently remark on the vibrancy and active growth of the local blogosphere, and report on new developments, particularly when blog discussions focus on issues of topical interest.

The Estonian Media Services Act[41] (§ 22) provides that persons who are involved in the media services sector may, at their own initiative, form associations and establish systems of self-regulation for setting voluntary standards of conduct and defining good practices. The rules and regulations applicable within such associations are determined by the members.

The **Estonian Newspaper Association** (EALL) has adopted the "Code of Ethics of the Estonian Press"[42] and an "Agreement of Best Practices of Online Comments (2008)".[43] Under those rules, newspapers may take any of a number of measures suitable for dealing with inappropriate comments, including word filters, blocking of IP addresses, and notification of the law enforcement authorities. The agreement has also been approved by online newspapers and supplemented by their own best practices guidelines.[44]

Private databases, internet platforms, blogs, and the like, normally publish general terms and conditions setting out the rights and duties of users with regard to data protection and the disclosure of information. The Estonian Data Protection Inspectorate regularly issues guidelines concerning the processing of personal data. Those guidelines also explain the terms and conditions applicable to the removal illegal internet content in accordance with the law.[45] Personal forums, websites, blogs and the various social media platforms usually provide, of their own accord, technical means for voluntarily blocking, filtering, or removing illegal or immoral content or deleting inappropriate account names. In cases involving defamation of character, cyberbullying, and other illegal activities,

---

41 Media Services Act (MSA), adopted 16 December 2010, entered into force 16 January 2011, English translation available at https://www.riigiteataja.ee/en/eli/511052015002/consolide.

42 Code of Ethics of the Estonian Press (in Estonian: Eesti *ajakirjanduseetika koodeks*), approved by general meeting of the Estonian Newspaper Association. English translation available at http://www.eall.ee/
code.html (8 November 2015).

43 Online *kommentaaride hea tava lepe*, available at http://www.eall.ee/lepped/online.html.

44 For example, the newspaper *Äripäev* adapted their own best practices for online comments, available at http://www.aripaev.ee/staatilised-lehed/kommentaaride-hea-tava.

45 English at http://www.aki.ee/en; Estonian at http://www.aki.ee/et/juhised.

it is possible to block a user's access or/and inform the administrator as to the illegal content of a posted comment. In most cases, the owners of forums, blogs, etc., inform users of their right to take down illegal comments, opinions, or other contributions containing illegal or defamatory remarks, hate speech, or illegal personal data.[46] There are exceptions, however, and not all social media platforms offer the possibility of changing or taking down inappropriate posts or of blocking or filtering the content of comments.

[46] See, for example, the conditions of the use of the forum "Family School" (*perekool*), available at http://www.perekool.ee/artiklid/toimetus/kasutajatingimused/.

Monitoring and protection of intellectual property rights

Estonian copyright protection organisations are authorised to monitor the internet and, if necessary, to request of ISPs that they remove illegal content (copyrighted works or other content subject to similar rights), or to bring legal action against ISPs or persons providing access to the content (CoA §§ 77 and 78). There are a number of organisations that work to represent and protect the interests of authors. Among them is the Business Software Alliance (BSA), a non-profit organisation devoted, among other things, to the protection of intellectual property rights and data protection. The website of the organisation provides information on a wide range of issues relating to intellectual property rights in software, including software piracy.[47]

The Estonian Authors' Society, a non-profit organisation established in 1991, is the largest writer's association in the country. In working to represent the members' interests, the Estonian Author's Society also contributes to efforts to combat copyright violations on the internet. According to a 2013 report by Freedom House,[48] "the removal of online content related to possible copyright infringement on YouTube and other video streaming services…was greatly facilitated by requests from copyright enforcement organisations representing Estonian authors". The report estimates that over the years more than 80,000 videos have been taken down from the internet, noting also that, "hundreds of videos have been removed from YouTube for copyright violations even though the authors themselves who were apparently not aware of the activities of copyright enforcement organisations representing their rights posted some of the videos". Concerning the sources of the complaints registered, the report has this to say: "All of these requests came from individuals or companies; the Estonian government has not issued any requests for removal of content on any of Google's platforms, including YouTube, since at least 2010.[49] However, this is not true for other platforms, for example in 2014 Facebook received 13 requests from Estonia relating to criminal cases either as requests for data or to restrict access to content."[50]

Child abuse and child pornography

Estonia implemented EU directive 2011/92/EU on combating sexual abuse and sexual exploitation of children, and child pornography in 2013; the respective amendments to the Estonian Penal Code and other statutes entered into force in December of that year. Estonia participates in Europol's EMPACT Operational Action Plan (OAP), and in its "Twins" Analysis Work File (AWF). As of 2014, Estonia also accepts reports from the National Centre for Missing & Exploited Children (NCMEC) on the online sharing of child abuse material (CAM) (other than via TOR or P2P).

"Web Constables"[51] is a website developed by the Estonian Police and Border Guard Board. Web constables is the term used for police officers who work over the internet (including through social media platforms, such as Facebook, Twitter and Rate), responding to reports and messages submitted over the internet concerning various matters, including sexual or other forms of abuse. They also provide training in internet security for both children and adults. There are currently three

---

47 See http://ww2.bsa.org/country/Report%20Piracy.aspx.

48 Freedom House, "Freedom on the Net 2013: Estonia", pp. 4-5, available online at https://freedomhouse.org/sites/default/files/resources/FOTN%202013_Estonia.pdf (accessed 9 December 2015) see also: "Preliminary report," Project 451, Institute of Digital Rights, available online at http://451.ee/en/preliminary-report/.

49 See the Google Transparency Report, "Estonia – Removal Requests," available at http://www.google.com/transparencyreport/removals/government/EE/.

50 Facebook, Government Request Report, available at https://govtrequests.facebook.com/country/Estonia/2014-H2/ (11 November 2015).

51 *Veebikonstaablid*, available at https://www.politsei.ee/en/nouanded/veebikonstaablid/ (8 November 2015).

web constables on the staff; as of 2013, there is one web constable assigned to dealing especially with the Russian-speaking public. According to Police and Border Guard Board statistics for the years 2012 and 2013, somewhat more that 5500 reports or messages were received in each of those years. The web constables' task is of an advisory nature; they do not themselves take police action. In practice, they are able to resolve many issues simply by providing the appropriate advice. When further action is necessary, however, they forward the relevant information to the appropriate police unit. Working with Facebook makes it possible to quickly remove CAM and to obtain data for identifying the party by whom it was uploaded.[52]

The police also work in cooperation with the Estonian Union for Child Welfare, which operates a free online service, "*Vihjeliin*" (www.vihjeliin.ee), providing internet users with a means to reporting on illegal or offensive material being distributed online – including images depicting the sexual abuse or exploitation of minors, minors in erotic or pornographic poses, child trafficking, and similar offences. Information can be submitted anonymously, and the personal details of the source are not investigated or recorded.

In addition to cooperating with law enforcement authorities, the Estonian Union for Child Welfare works closely with other national organisations, including internet service providers and non-profit organisations, and such international networks as INSAFE and INHOPE. Cooperation between the online notification service "*Vihjeliin*" and the INHOPE network allows for faster and more efficient information exchange concerning child abuse websites. Between 1 April and 30 September 2014, a total of 34 reports were received concerning images depicting the sexual abuse of children, and 506 reports concerning pornographic images of adults (aged 18 or over).[53] The Estonian Union for Child welfare is also working to create and manage a national STOP-list, and to raise awareness on the part of telecommunication companies for the importance of restricting access to CAM web sites.

Other possibilities are also available for young people to share their problems and seek advice or help. Thus, for example, the website "*Lapsemure*"[54] provides a forum for youthful internet users where thy can discuss their concerns and difficulties, and find information on the subject of illegal internet content. The Estonian Advice Centre (www. lasteabi.ee), in addition to providing online counselling, also operates the round-the-clock "Child Helpline", available at the European telephone hotline number 116 111.

"Smartly on the Web" (formerly "Safer internet") or, *Targalt internetis* (www.targaltinternetis.ee), is the outcome of a special project co-financed by the European Commission's Safer Internet Programme, which provides training for children, teachers, and parents in best practices with regard to the safe, secure, and appropriate use of the internet and other digital communication technologies. Among other things, it also organises media campaigns and events to raise public awareness for the issues, working in cooperation with various authorities and NGOs, including the Estonian Union for Child Welfare, the Estonian Advice Centre, and the Information Technology Foundation for Education, the Digital Innovation Centre *Tiigrihüpe*, and the Police and Border Guard Board.

Cyber security and monitoring

A study recently published by the Washington-based Business Software Alliance describes the cyber security situation in Estonia as follows: "Estonia was one of the first countries to develop a national

---

52 See further: "Global Alliance Against Child Sexual Abuse Online – 2014 Reporting Form, Estonia", available at http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organised-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_estonia_en.pdf.

53 For the statistics, see http://vihjeliin.targaltinternetis.ee/en/statistika/.

54 http://www.lapsemure.ee/?tutvustus.

cyber security strategy in 2008, followed by the release of an updated strategy in 2014. The country also has a wide range of legislation that covers information security and cyber security. Estonia has a well established CERT, CERT Estonia, under the control of the Information System Authority. Further to national bodies, is also notable that NATO's Cyber Security Centre of Excellence is based in Estonia. While no formalized public-private partnerships exist, public entities do work closely with relevant private-sector organisations."[55] Closer public-private collaboration was initiated in 2006, with the signing of a memorandum of understanding between the largest telecommunications service providers and commercial banks, and the Ministry of Economic Affairs and Communications, for the launching of "Computer Security 2009", described as "a collaboration project intended to enhance the security of public and private e-services and to promote public awareness about protecting information systems".[56] Public-private collaboration was also reflected in the Estonian Cyber Security Strategy, adopted in May 2008, one year after a series of attacks against the Estonian information infrastructures. In keeping with that strategy, in 2011, a separate Cyber Defence Unit was created within the existing structure of the Estonian Defence League, a voluntary national military defence organisation, first established in 1918 and reconstituted in 1999 by the Estonian Defence League Act.[57] The stated mission of the Cyber Defence Unit is "to protect Estonia's high-tech way of life by protecting information infrastructure and supporting the broader objectives of national defence".[58]

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

Constitutional guarantees

In Estonia, freedom of speech and free access to information are guaranteed by the Constitution, which provides in § 44, para. 1, that every individual has a right to have free access to information disseminated for public use. The right to "freely disseminate ideas, opinions, beliefs and other information by word, print, picture or other means" is affirmed in § 45. Circumscription of that right by law is permitted in order to "protect public order, public morality, and the rights and freedoms, health, honour and good name of others". It may also be restricted for "public servants employed by the national government and local authorities, and in order to protect a state secret, trade secret or information received in confidence which has become known to the public servant by reason of his or her office; and to protect the family and private life of others, as well as in the interests of the administration of justice". There is also a specific statutory duty to provide free access to public information through internet.[59]

Estonian court practice in this area follows the precedents established by the case law of the European Court of Human Rights (ECHR). This is in keeping with rulings by the Estonian Supreme

---

55 BSA: The Software Alliance, "EU Cybersecurity Dashboard: A Path to a Secure European Cyberspace", p. 12; available online at http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf.

56 '*Arvutikaitse 2009' koostööleping* (Memorandum of Understanding for 'Computer Security 2009'. Tallinn, 23 May 2006, p. 7, available online at http://www.arvutikaitse.ee/wp-content/uploads/2006/12/arvutikaitse2009_lepingu_tekst.pdf.

57 Ibid., pp. 8-9; see also *Seletuskiri Vabariigi Valitsuse määruse "Vabariigi Valitsuse määruste muutmine" eelnõu juurde* (Explanatory Memorandum to the draft regulation on amending certain government regulations), 22 November 2010. http://eelnoud.valitsus.ee/main#TnXRXqdL;Valitsus asutas Kaitseliidu küberkaitseüksuse. Kaitseministeerium, 20 January 2011, http://www.kmin.ee/et/valitsus-asutas-kaitseliidu-kuberkaitseuksuse.

58 The Estonian Defence League's Cyber Unit. The Defence League, http://www.kaitseliit.ee/en/cyber-unit.

59 Public Information Act § 33: "Every person shall be afforded the opportunity to have free access to public information through the internet in public libraries, pursuant to the procedure provided for in the Public Libraries Act."

Court to the effect that, with regard to statutory provisions being applied for the first time, it is incumbent upon Estonian courts to take into account the court practice of the European Court of Human Rights, the European Court of Justice, and the courts of Member States whose legal systems are comparable to that of Estonia.[60] There is no constitutional court in Estonia; the constitutionality of laws and other legislation of general application is reviewed by the Constitutional Review Chamber of the Supreme Court. Constitutional review cases are adjudicated by the Supreme Court either at the sessions of the Constitutional Review Chamber or sitting *en banc*. The Court is vested with the power to declare any law or other legislative enactment wholly or partially invalid where it is found to be contrary to the spirit or the letter of the Constitution.

According to ECHR precedent, the imposition of limitations on freedom of speech and free internet access may be considered as justified where there exists a pressing social need for such a measure (*Vogt v. Germany*, no.17851/91), and where it is proportionate to the legitimate aim pursued (*Observer and Guardian v. the United Kingdom*, 13585/88). Statutory provisions that provide for exceptions to guaranteed rights must to be narrowly interpreted (*Klass and others v. Germany*, no. 5029/71), and the necessity for restricting such rights must be convincingly established (*Autronic AG v. Switzerland*, no. 12726/87). While only a small number of cases touching on these issues have thus far been brought before the Estonian courts, it is safe to say that these fundamental principles have, as a general rule, been adhered to in Estonian legislation and legal practice.

Legal foreseeability, availability of remedies, proportionality test

In general, the Estonian statutes governing the liability of ISPs for illegal internet content **meet the qualitative requirements** developed by the European Court of Human Rights. Thus, in *Delfi AS v. Estonia* (App. no. 64569/09) the European Court of Human Rights (Grand Chamber) held as follows:

> "…the Court is satisfied on the facts of this case that the provisions of the Constitution, the Civil Code (General Principles) Act and the Obligations Act, along with the relevant case-law, made it foreseeable that a media publisher running an internet news portal for an economic purpose could, in principle, be held liable under domestic law for the uploading of clearly unlawful comments, of the type at issue in the present case, on its news portal" (p. 128).

Before stating this conclusion, however, the Court pointed out that although legal certainty is to be desired, there may a need for the use of terms "which, to a greater or lesser extent, are vague" in order "to keep pace with changing circumstances". The statutes named in the judgment (the General Part of the Civil Code Act, and the Law of Obligations Act) follow the German model, constituting in the aggregate a code of civil law. Tort liability is dealt with in the LOA (§§ 1043ff.), based on the notion of legally protected rights, and the prevailing doctrines have been developed in the case law and legal literature. The provisions on the liability of ISPs are modelled on those of Directive 2000/31/EU, which are quite clear with regard to the different functions performed by ISPs and differences in the degree of liability borne by ISPs depending on the functions at issue. A full assessment of the relevant statues is hardly possible at this point, due both to the lack of court precedents and to the absence of general public discussion of the rights affected by any imposition of restrictions on freedom of expression in internet. The use of such general terms, as "predominant public interest", "excessive damage to the rights", "justified reasons" reduces the foreseeability of legal consequences.

While there also exists a statutory basis for seeking the blocking or removal of illegal content from the internet (LOA § 1055), there are no clear rules on the blocking and filtering of internet content as ***remedies*****.** In this area, it is possible that Estonian law does not satisfy the qualitative criteria developed by the European Court of Human Rights, due to the absence of clear and qualified

[60] In civil matters, this was declared to be the case by the Supreme Court of Estonia as early as 2004.

grounds and procedures for the use of such measures as the blocking, filtering, or removal of illegal internet content. Thus, for example, in *Liivik v. Estonia*, the ECHR found that the "insufficient clarity and foreseeability" of the law applied by the Estonian courts were valid grounds granting the applicant's claim.[61] Conversely, in *Delfi AS v. Estonia* the ECHR found that adequate statutory remedies had been provided for, noting that under Estonian law "…the injured person had the choice of bringing a claim against the applicant company or the authors of the comments…" (p. 151). Despite the technical or other obstacles that might prevent disclosure of the identity of a person who posted illegal content, the possibility of bringing suit against the company that provided internet access was found to be a sufficient remedy. In this context, the ECHR also draws attention to its judgment in *Krone Verlags GmbH & Co. KG v. Austria*[62], where it had found that "shifting the risk of the defamed person obtaining redress in defamation proceedings to the media company, usually in a better financial position than the defamer, was not as such a disproportionate interference with the media company's right to freedom of expression".

Estonian law also provides remedy in cases where inaccurate information has been published on the internet. LOA § 1047, para. 4 provides that "in the case of the disclosure of incorrect information, the victim may demand that the person who disclosed such information refute the information or publish a correction at the person's expense regardless of whether the disclosure of the information was unlawful or not". The correction of incorrect data may be also be ordered under the terms of the Personal Data Protection Act (PDPA) § 6, para. 7, and §§ 21 and 24. The removal of incorrect data may be ordered in reliance on PDPA § 24, para. 5.

In cases reviewed by the Supreme Court, the arguments of legality, precision, necessity, adequacy and proportionality, and the need to respect international human rights standards have been repeatedly raised and elaborated on. Work is currently underway to bring Estonian law into conformity with the European Council Framework Decision of 28 November 2008 2008/913/JHA[63] on "combating certain forms and expressions of racism and xenophobia by means of criminal law" by establishing a framework for the criminalisation of hate speech in the country. Estonia is now the only country in the EU where hate speech is not considered a criminal offence. A draft proposal for an amendment to § 151 of the Penal Code, prepared by the Ministry of Justice as early as 2008,[64] has

---

61 In *Liivik v. Estonia*, App. no. 12157/05 (ECtHR, 25 June 2009), the reason given for applying to the European Court of Human Rights was that the sentence had been based on an unclear and incomprehensible law and was thus in violation of art. 7, para. 1 of the CHR. The European Court of Human Rights, having assessed the background against which the offence was committed, concluded that the interpretation and application of the domestic law did not meet the standards of clarity and foreseeability required under the Convention.

62 See *Krone Verlags GmbH & Co. KG v. Austria (no. 4)*, no. 72331/01, at 32, 9 November 2006.

63 EUR-Lex, "Access to European Union Law," accessed May 5, 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008F0913:en:NOT (8 November 2015).

64 Article 151 of the Penal Code (15 September 2015) reads as follows:
"§ 151. Incitement of hatred
(1) Activities which publicly incite to hatred, violence or discrimination on the basis of nationality, race, colour, sex, language, origin, religion, sexual orientation, political opinion, or financial or social status if this results in danger to the life, health or property of a person is punishable by a fine of up to three hundred fine units or by detention.
(2) The same act, if: 1) it causes the death of a person or results in damage to health or other serious consequences; or 2) committed by a person who has previously been punished by such act; or 3) [repealed - RT I, 23 December 2014, 14 - entered into force 1.1.2015] is punishable by a pecuniary punishment or up to three years' imprisonment.
(3) An act provided for in subsection (1) of this section, if committed by a legal person, is punishable by a fine of up to 3200 euros.
(4) An act provided for in subsection (2) of this section, if committed by a legal person, is punishable by a pecuniary punishment."

recently come under discussion again among stakeholders and in the media. The main concern expressed by stakeholders and legal experts is that the definition of hate speech contained in the draft amendment is too broad and not sufficiently clear, so that there is a risk that it could become an obstacle to guaranteeing freedom of expression and the freedom of the media. In general, there is little support for the proposed amendment.

Data protection

There are a number of judgments issued by the Estonian Supreme Court in which the limits to freedom of expression in connection with the publication of sensitive personal data are defined. There is, however, no case law relating to any court order requiring the blocking of internet service, restrictions on access to content, or the filtering of content. Similarly, there have been no copyright cases in which the filtering, blocking or taking-down of illegal content was at issue. In rare cases – involving defamation or violations of data processing rules – the Supreme Court has upheld an order to take down illegal internet content or established the legality of an administrative request made by a government agency.[65] In those cases the Estonian Supreme Court has adhered to the principles followed in the practice of the ECHR in cases involving the removal of illegal internet content.

The "duties and responsibilities" of journalists with regard to the publication of false information on the internet were a matter of discussion in a 2010 Supreme Court judgment.[66] The case concerned the publication in the online newspaper *Eesti Päevaleht*, on 4 January 2008, of an article headlined "Well-known Bankruptcy Trustee among the KGB spies". The person wrongly identified by the Security Police Board as a KGB agent had the same name as the true KGB agent. That the persons involved were, in fact, two separate individuals could easily have been verified. The article was publicly accessible through links provided by the online search engines Google, AltaVista, and Yahoo. The Supreme Court ordered the news portal to submit an application to the search engines in question for removal of the links from their systems in order to prevent the dissemination of false and defamatory content.

For a person who wishes to obtain a court order for the removal of illegal internet content, the simplest and most direct method is to file a claim against the service provider. However, in cases where the service provider is not the party that published the content in question, the question arises as to whether the defendant can be compelled to remove internet content, or to stop the publication of incorrect information, where the information sources are not under the defendant's control. Thus, for example, in a case involving the publication of defamatory articles on four internet portals (www.tallinnapostimees.ee, www.delfi.ee, www.ohtuleht.ee and www.irl.ee), the plaintiff's complaint was dismissed by the lower court on the grounds that the sites where the articles were published were not under the control of the defendant (judgment of 25 September 2013, in civil case

---

65 There are only two judgments directly concerned with the removal of illegal internet content. The first is from 10 June 2009, in the Delfi AS case (civil case no. 3-2-1-43-09), concerning the removal of defamatory comments from internet, and will be analysed below in section 5). The second is the judgment from 12 December 2011 in administrative case no. 3-3-1-70-11, and concerns a request to terminate the communication of personal data. The Data Protection Inspectorate ordered the company EMT AS to terminate the communication of personal data relating to an complainant's creditworthiness. EMT refused and filed a petition to have the order issued by the Data Protection **Inspectorate** vacated**.** The court ruled that the processing of personal data to be communicated to third persons for assessing the creditworthiness of persons, or for other such purposes, is, in principle, permitted, even without the consent of the persons in question. In the specific case, however, the communication of personal data still on record in Estonian Credit Register more than 13 years after a breach of contract had occurred, was found to excessively damage the legitimate interests of the data subject. The petition was therefore rejected.

66 Judgment of the Estonian Supreme Court of 9 December 2010 in civil case no. 3-2-1-127-10. See also *Schuman v. Poland* (dec.), no. 52517/13, 3 June 2014.

no. 3-2-1-80-13, p. 27). Ruling on an appeal of that judgment, the Estonian Supreme Court concluded that, in principle, the fact that a party has no direct control over an internet site does not render it immune from claims seeking the removal of illegal content from the site in question. A service provider that provides the means for transmission of illegal content can perform its obligation to remove the illegal content by instructing the owner of the site to do so. In such cases, the court judgment will replace the defendant's statement of intention to remove the data on the website (§ 68, para. 5, of the General Part of the Civil Code Act, in conj. with § 184, para. 1 of the Code of Enforcement Procedure), even where the defendant is not itself the owner of the website. The Supreme Court has also ruled that § 1055, para. 1, of the LOA may serve as the statutory basis for claims seeking to compel the defendant to instruct the owner of a website to remove defamatory content or incorrect information.[67]

Overall, it may be assumed that the use of broadly defined terms in the laws will allow the courts sufficient discretionary authority to apply the law in new situations and to take into account technological developments. At the same time, however, somewhat more precision is needed in order to meet all of the requirements and principles – particularly those of legal certainty and foreseeability – formulated in the case law of the ECHR.

Delfi AS v Estonia [68]

A new paradigm for participatory online media was created by the ECHR judgment in the *Delfi AS v. Estonia* case, in which the Court obliged online news platforms to filter or monitor certain kind of users' comments for content of an extreme nature in order to prevent possible liability.

Delfi is one of the largest news portals in Estonia. Readers may post comments on news stories, although Delfi does have policies in place to limit unlawful content, including the installation of an automatic filtering system and an integrated notification and take-down system. Delfi ran a story concerning ice bridges between the Estonian mainland and the islands, which were damaged by ferries belonging to a company owned by the local businessman L. Six weeks after publication, L requested that some 20 comments be deleted, and sought damages. Delfi removed the offending comments the same day, but refused to pay damages. L went to court and damages were awarded.

Delfi claimed to be a neutral intermediary and therefore immune from liability under the EU's e-Commerce Directive regime. The Estonian Supreme Court rejected this argument in its decision of 10 June 2009[69]. Delfi then brought the matter to the European Court of Human Rights and lost the case in a unanimous chamber decision. Bringing the matter before the Grand Chamber in 2015, it again failed, this time by a vote of 15 to 2.[70]

Delfi's argument before the ECHR was that there was no legal basis for interfering with its right to freedom of expression – including the right to store information and to enable users to share their opinions. It submitted that there was no statute or case law stating that an intermediary was to be considered as the publisher of content of which it was not aware. Quite to the contrary, it claimed, applicable law expressly prohibited the imposition of liability on service providers for third-party content. In this connection, the applicant company referred to the Directive on Electronic Commerce,

---

67 Judgment of the Estonian Supreme Court of 9 December 2010 in civil case no. 3-2-1-127-10, p. 11.

68 ECHR 10 October 2013, 64569/09, *Delfi vs. Estonia*. T.E. Synodinou, "Intermediaries' liability for online copyright infringement in the EU: Evolutions and confusions", 2015 (31) 1 *Computer Law & Security Review*, pp. 57-67.

69 Judgment of the Estonian Supreme Court of 10 June 2009 in civil case no. 3-2-1-43-09, available in Estonian at http://www.riigikohus.ee/?id=11&tekst=RK/3-2-1-43-09 (8 November 2015), abstracted by the Grand Chamber, loc. cit., at 41-43.

70 ECHR (Grand Chamber), 16 June 2015, 64569/09, *Delfi AS v. Estonia*.

the Estonian Information Society Services Act and the Council of Europe Declaration on freedom of communication on the internet and other acts. These provided for limited and knowledge-based liability for illegal content, it submitted. Under those rules, service providers were exempted from liability where, upon obtaining actual knowledge of illegal activities, they acted expeditiously to remove or disable access to the information concerned. The applicant company further argued that even the existing tort law did not classify disseminators (postal workers, libraries, bookstores and others) as publishers. Thus, it remained entirely unclear how the existing tort law had been applied to a "novel area related to new technologies" as held in the Chamber judgment. Furthermore, Delfi AS claimed that the affirming of the liability would not be necessary in a democratic society, since it had a "chilling effect" on freedom of expression; it amounted to the establishment of an obligation to censor private individuals and that there was no pressing social need for a strict liability standard for service providers.

The Court notes at the outset that user-generated expressive activity on the internet provides an unprecedented platform for the exercise of freedom of expression. That is undisputed and has been recognized by the Court on previous occasions (see *Ahmet Yıldırım v. Turkey*, no. 3111/10, art. 48, ECHR 2012, and *Times Newspapers Ltd (nos. 1 and 2) v. the United Kingdom*, nos. 3002/03 and 23676/03, art. 27, ECHR 2009). The Court considers also "that because of the particular nature of the internet, the "duties and responsibilities" that are to be conferred on an internet news portal for the purposes of Article 10 may differ to some degree from those of a traditional publisher, as regards third-party content." (p.113) The Chamber considered that "the news article published by the applicant company that had given rise to the defamatory comments had concerned a matter of public interest and the applicant company could have foreseen the negative reactions and exercised a degree of caution in order to avoid being held liable for damaging the reputation of others. However, the prior automatic filtering and notice-and-take-down system used by the applicant company had not ensured sufficient protection for the rights of third parties. Moreover, publishing news articles and making readers' comments on them public had been part of the applicant company's professional activities and its advertising revenue depended on the number of readers and comments."

Consequently, the Court limited the applicability of the case to "duties and responsibilities" of internet news portals, when they provide for economic purposes a platform for user-generated comments on previously published content and some users – whether identified or anonymous – engage in clearly unlawful speech, which infringes the personality rights of others and amounts to hate speech and incitement to violence against them. In any event, the Chamber was not convinced that measures allowing an injured party to bring a claim only against the authors of defamatory comments would have guaranteed effective protection of the injured parties' right to respect for their private life. "It had been the applicant company's choice to allow comments by non-registered users, and by doing so it had to be considered to have assumed a certain responsibility for such comments. For all the above reasons, and considering the moderate amount of damages the applicant company had been ordered to pay, the restriction on its freedom of expression was considered to have been justified and proportionate. There had accordingly been no violation of Article 10 of the Convention (p 65)."

The author of the report notes that the Grand Chamber judgement has had certain practical consequences:

1) News portals in Estonia today, more often than not, foreclose the whole commenting platform for articles reporting on controversial issues that could give rise to extreme comments (e.g., on subjects such as the European migration crisis, same-sex marriage, etc.), or where a moderator discovers a comment that resorts to hate speech;

2) Delfi has disclosed that they have changed their working processes and hired additional moderators to exercise stricter supervision over the content of comments;
3) there still remain possibilities for submitting anonymous comments; in addition, all the major Estonian online publishers have appended to each comment in their comment sections a link "Report an inappropriate comment";
4) current policy is that the owners of the portal remove offensive content from comments immediately upon receipt of notice thereof.

The steps taken by the news portals can be seen as a clear attempt by them to adapt their operations in accordance with the Grand Chamber's ruling that such portals have an obligation to monitor user-generated content in order to prevent the publication of defamatory statements.

It is noteworthy that the reasoning behind this judgment would appear to be that speech must be justified in order to evade liability. In this, the Grand Chamber seems to give little regard either to its own case law about political speech, or its repeated emphasis on the importance of the media in society. Given the extremely low damages awarded, the case did not open the floodgates in Estonia and, consequently, is unlikely to result in significant adverse consequences for intermediaries or for free speech in general.

Public discussion concerning Delfi case in Estonia

The first scholarly treatment of the Delfi case was published in the Estonian legal journal *Juridica* (in Estonian) by K. Turk, the lawyer who represented Delfi before the ECHR.[71] Turk expressed neither criticism nor support for the decision, but focused rather on the question of whether the identification of users can be used to find a just balance between the rights potentially being violated, the freedom of expression of internet users, and the freedom of enterprises that mediate internet services. The internet, she argues, is a symbol of privacy and an opportunity for users to send and receive messages under the cover of overall anonymity. She takes the view that only anonymity will ensure people's willingness to participate in public debate on controversial topics. No other studies on the case have been published by Estonian scholars. Following publication of the judgment, concern focused primarily on the future of Estonian internet media, where comments were hitherto considered highly welcome and were not censored or filtered. The 2015 judgment of the Grand Chamber has given rise to concerns that liability for hate-speech has been shifted onto the media and away from the actual commenters. On the one hand, making the media channels responsible for hate speech published by users has allowed users, who before the decision were afraid of harassment by anonymous commenters, to express themselves more freely. At the same time, however, there has been a perceptible rise in the "hate factor" evidenced in online comments being posted in Estonia. Whether this is attributable to a sense of impunity created by the judgement, or is more a reflection of the general socio-political context (e.g., European migration crisis; rise of nationalism, etc.), is a question that requires further analysis.

Irene Kull[72]
15.11.2015

Revised on 03.05.2016 taking into consideration comments from Estonia on this report

[71] K. Turk, *Digitaalkeskkonnas isiku tuvastamise meetmete poolt ja vastu*, 2014 (3) Juridica, pp. 175 – 188.

[72] Irene Kull is professor of civil law at the University of Tartu, Estonia.