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 521-538

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.

POLAND

1. Legal Sources

There is **no specific legislation concerning blocking, filtering and take-down of illegal Internet content** in Poland.

The obligation to block or take-down the illegal content can, however, **derive from the decision of a court or a public administration body** which is based on the applicable law. The decision must be addressed to the content providers or to the Internet service providers considered as the "aiding" person under the relevant law (in this regard see section 3 below).

In this context it should be mentioned that the Constitution of the Republic of Poland guarantees the **freedom of expression.**[1] This means that each Polish citizen has the right to **express his/her views and opinions** and to **acquire and disseminate the obtained information** (also via Internet). Thus, the freedom of expression guarantees the prohibition of censorship. The freedom of expression is not, however, unlimited. Each limitation of this principal personal right must, however, result from a particular written law (such as Penal Code or Civil Code) enacted by the Parliament (wider analysis in this regard is provided in section 5.2 below of this report).

With regard to Internet service providers (especially access providers and hosting providers), it should be mentioned that since the Polish legislator implemented **the European Directive 2000/31/EC on electronic commerce** (hereinafter referred to as "E-Commerce Directive")[2] in the domestic legal system by way of **the Act on Providing Services by Electronic Means**, ISPs' liability is possible only in cases indicated in the latter regulation. The provisions of the Act (Art. 12 – 14) create specific exemptions from liability for ISPs providing mere conduit, caching and hosting services (the particular regulations are discussed in section 2.1. and 2.2. below).

ISPs can potentially bear liability on the ground of various **civil, criminal or administrative regulations which can be a legal basis for claims of blocking or removing the content** (against hosting providers or – more rarely – access providers). The particular provisions of civil, criminal and administrative law that could provide the grounds for an ISP's liability are listed in section 2 below. However, since the provisions on exclusion of ISPs' liability concern all areas of law, i.e. civil, criminal and administrative law, the ISP can bear the liability solely in case the exceptions from liability (art. 12-14) do not apply. Therefore, in order to hold the ISP liable for the illegal - stored or transmitted – Internet content, in each case the court must take into consideration both:

- the provisions of particular substantive law (for example, the Penal Code) and
- the regulation of the Act on Providing Services by Electronic Means (i.e. related to both civil, criminal and administrative law).

The following international standards relating to illegal Internet content have been transposed into the Polish legal system. **The Convention on Prevention of Terrorism of the Council of Europe**[3] came into force in Poland on 1 August 2008. The **Cybercrime Convention of the Council of Europe**[4]

---

1 Constitution of the Republic of Poland Section 54.

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

3 Convention on Prevention of Terrorism, Warsaw (16.05.2005): http://conventions.coe.int/Treaty/EN/Treaties/Html/196.htm.

4 Convention on Cybercrime, Budapest (23.11.2001): http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

entered into force in Poland on 1 June 2015. Furthermore, Poland has assented to the **Additional Protocol** concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems.[5] On 1 June 2013, the **Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse of Council of Europe**[6] came into force in Poland.[7] On 1 September 2002, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data entered into force in Poland.[8]

2. Legal Framework

As already mentioned, in order to hold the ISP (rendering such services as hosting, caching and mere conduit) liable for the illegal Internet content, the court must (i) conclude that the ISP's activity can be considered as breaching the substantive domestic law (criminal, civil or administrative); (ii) conclude that the exceptions from liability included in art. 12-14 do not apply to the ISP. Therefore, the ISP can bear the liability solely where both abovementioned conditions are met.

Thus, ISPs can potentially bear liability on the ground of various civil, criminal or administrative regulations; this can then be a legal basis for claims of blocking or removing the content. The particular provisions in this regard are presented below.

Criminal Law Provisions

Under Polish criminal law there are several offences concerning the illegal content of information that can be committed via Internet. These offences are related to both **personal rights infringements** as well as **dissemination of information prohibited by law**.[9]

In light of the Polish Penal Code, imputing to another person, a group of persons, an institution or organisational unit such **conduct, or characteristics that may discredit** them in the face of public opinion or result in a loss of confidence necessary for a given position, occupation or type of activity (defamation) is prohibited.[10] What is more, if the perpetrator commits the offence through the mass media (such as, for instance, the Internet) the stipulated sanctions are stricter.[11]

Insulting another person in his/her presence, or though in his/her absence but in public, or with the intention that the insult shall reach such a person is also prohibited.[12] The stipulated sanctions are stricter if the **insult is made via mass media** (e.g., the Internet).[13]

---

5 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems http://conventions.coe.int/Treaty/en/Treaties/Html/189.htm.

6 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) http://conventions.coe.int/Treaty/EN/treaties/Html/201.htm.

7 Transposition of the conventions into the Polish legal system was performed by appropriately amending certain domestic Acts. In particular, the Cybercrime Convention and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse were transposed into the Penal Code, the Act on Police and the Act on the Educational System. The Convention on Prevention of Terrorism was transposed to the Act on the Prevention of Money Laundering and the Prevention of the Financing of Terrorism.

8 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (28.I.1981): http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

9 M. Sawicki, Przestępstwa związane z treścią informacji*, Edukacja Prawnicza* 2012 No. 10 p. 25-29.

10 Penal Code Section 212.1.

11 Penal Code Section 213.2.

12 Penal Code Section 216.1.

13 Penal Code Section 216.2.

The Polish Criminal Code further prohibits the making of **a threat to another person** to commit an offence detrimental to that person or detrimental to his/her next of kin, and if the threat causes a justified fear to the threatened person that it will be carried out.[14]

The person who imports or **propagates pornographic material in which minors participate**, or **pornographic material associated with the use of violence or the use of an animal** can also be held liable.[15]

The Polish Penal Code moreover lays down general provisions concerning liability for **public promotion of a fascist or other totalitarian system of state** and for **hatred speech** based on national, ethnic, race or religious differences or for reason of lack of any religious denomination.[16] There is also a prohibition against the **publicl insulting of** a group within the population or a particular person because of his national, ethnic, race or religious affiliation or because of his/her lack of any religious denomination.[17]

There are also some criminal provisions **in separate regulations** concerning the offences related to illegal content. In this regard the following legal regulations can be mentioned:

a) Under the Polish Act on Counteracting Drug Addiction, the **advertising and promoting drugs**, including acting via the Internet, is prohibited.[18]
b) According to the Polish Act on Combating Unfair Competition, disclosing **to another person information that is a business secret is prohibited.**[19]
c) In light of the Polish Act on Copyright and Related Rights[20] every person who, without authorization or against its terms and conditions, **disseminates someone else's work**, in the original or derivative version, performance, phonogram, videogram or broadcast shall be held liable.
d) Under the Polish Act on Industrial Property Rights[21] marking goods with a counterfeit trademark for the purpose of placing them on the market or **placing on the market goods bearing such trademark** is forbidden.
e) The Polish Act on Personal Data Protection[22] lays down the provision concerning liability for **disclosure of personal data or providing access to them** by unauthorized persons.
f) In accordance with the Polish Fiscal Penal Code[23] the **organization and promotion of gambling, including promotion via the Internet, is banned**.

In order to **prevent further crime,** the Polish Penal Code provides that **the objects (including websites) that were used or were intended to be used in a criminal act or produced by a criminal act can be confiscated** (the forfeiture of items directly derived from an offence). Therefore, **removing the illegal content or blocking the access to websites** can be ordered by a court.[24]

---

14 Penal Code Section 190.
15 Penal Code Section 202.
16 Penal Code Section 256.
17 Penal Code Section 257.
18 Act on Counteracting Drug Addiction Section 68 in conjunction with Section 20.
19 Act on Combating Unfair Competition Section 23.
20 Act on Copyright and Related Rights Section 116.
21 Act on Industrial Property Rights Section 305.
22 Act on Personal Data Protection Section 51.
23 Fiscal Penal Code Part 9.
24 Penal Code Section 44.

Civil Law Provisions

The Polish Civil Code lays down the provisions providing for the **protection of personal rights of a human being**, in particular rights such as health, freedom, dignity, freedom of conscience, name or pseudonym, image and privacy of correspondence. According to this regulation any person whose personal interests are threatened by another person's actions may **demand the actions be ceased** unless they are not unlawful. In case of infringement, he/she may also demand that the person committing the infringement performs the **actions necessary to remove its effects**. Doctrine and judicature indicate the various means that can be used to fix these effects, depending on the type of infringed rights, primarily by removing the state of violation, e.g. by destroying the false opinion or objects used to violate the personal rights. It should be emphasized that the court should strictly specify in the judgment the steps required to be made.[25]

Under the **Act on Combating Unfair Competition**, the entrepreneur whose interest is threatened or infringed by an act of unfair competition (such as e.g., infringement of the business secrecy or unfair or prohibited advertising) may **request relinquishment of prohibited practices or removal of the effects of prohibited practices**. The **court**, upon a motion of the entitled party, may also adjudicate on advertising materials and another items directly connected with commitment. In particular, the **court may order their destruction**.[26]

The Polish Act on Copyright and Other Rights provides for the regulations relating to **both moral and economic rights of the author**. First of all, the author whose moral rights have been threatened by actions of others, may **request such actions be ceased**. Where an infringement is committed, the author may also request that the person who committed the infringement should perform all the **actions necessary for the elimination of its effects.**[27] The author may also request from the person who infringed his economic rights to **cease such infringement and to eliminate its effects.**[28] Similar possibilities are provided in the Polish Act on Industrial Property Rights.

On the basis of the decisions of Polish courts, it can be interpreted that under civil law there are **two main options open to the injured party which are aimed at removing or blocking the illegal content by the ISP:**[29]

1. The court can order in the judgment that **the ISP removes or blocks the access to the content**, provided, however, that the provider was liable for the infringement in light of the provisions of the Act on Providing Services by Electronic Means (i.e. the provider had knowledge of the illegal content and did not make the access to this content impossible). This solution demands the suing of the ISP (instead of or together with suing the content provider).
2. In cases where only the content provider was sued, the court may **order the defendant** (i.e. content provider) **to notify to the service provider** (i.e., an operator of the web portal) the final court judgment that was given in a dispute between the injured party and the defendant and that provided that the uploaded content was unlawful. After having received such information, the ISP may no longer benefit from the liability exclusion regulations provided in the Act on Providing Services by Electronic Means and would need to remove the content in order to exclude its liability for the stored data being the subject of the court's judgment.

Administrative Law Provisions

---

25 Supreme Court Judgment dated 22 December 1997. II CKN 546/97.

26 Act on Combating Unfair Competition Section 18.

27 Act on Copyright and Other Rights Section. 78.

28 Act on Copyright and Other Rights Section 79.

29 Supreme Court Judgment dated 19 January 2015, II CSK 747/13.

Some legal acts provide for provisions which can be the basis for administrative decisions of public authorities to cease the breaches concerning illegal Internet content.

According to the Polish Act on Personal Data Protection,[30] in cases of a breach of the provisions on personal data protection, **the Polish Data Protection Authority, the so-called DPA** (*Generalny Inspektor Ochrony Danych Osobowych*; the Inspector General of Personal Data Protection) is entitled to, ex officio or upon a motion of a person concerned, by means of an administrative decision, **order to restore the proper legal state**, and in particular, *inter alia*, **to remedy the negligence**, **not to disclose personal data** or **to erase the personal data**. The breach of the applicable regulations may concern the unauthorized disclosure of personal data via the Internet.

According to the Act on Competition and Consumer Protection[31] **the President of the Office of Competition and Consumer Protection** shall issue a decision on pronouncing a practice as violating collective consumer interests and **ordering that the same be discontinued**, if he identifies a breach of the prohibition such as infringement of the business secrecy or unfair or prohibited advertising.

Under the Polish Broadcasting Act, the provision to the general public of on-demand audiovisual media services (i.a. the video-on-demand Internet services) that contain, as part of the catalogue of services, programmes or other broadcasts threatening the physical, mental or moral development of minors, in particular those containing pornography or exhibiting gratuitous violence without applying technical security measures or other appropriate measures to prevent minors from the reception thereof is prohibited. In cases of infringement of this regulation, **the Chairman of the National Broadcasting Council** may, acting by virtue of the National Broadcasting Council's resolution, issue a decision **ordering the media service provider to cease the practices, referred to as provision of media** services, if they infringe upon the provisions of the Act.

2.1. Blocking and/or filtering of illegal Internet content

2.1.1. Specific regulations

As has already been mentioned, currently **there are no specific legal regulations imposing the obligation to block or filter illegal Internet content** under Polish law.

It should, however, be mentioned that **the political proposals** regarding implementation to the Polish legal system of regulations concerning obligations on blocking the Internet content by access providers have been recently presented. The following concepts were widely discussed in this regard:

- A few years ago the Ministry of Finance prepared a draft of amendments to the telecommunication law according to which **the Registry of Prohibited Websites and Services was to be established.**[32] According to the proposed regulation, the prohibited site or service was to be recorded in the registry at the request of the authorized entity or the Customs Service, provided that it concerns: (i) content propagating fascist or other totalitarian regimes; (ii) pornographic materials related to minors, pornography materials related to presentation of violence or the use of animal or pornographic content containing manufactured or processed image of a minor participating in sexual activity; (iii) content, the presentation of which, allows the deceptive misleading of a person in order to achieve financial gain through extortion of information that

30 Act on Personal Data Protection Section 18.

31 Act on Competition and Consumer Protection Section 26.

32 The draft of the Act of the Amendment of the Act on Gambling and Certain Other Acts, 13th November, 2009, available at: http://www.archbip.mf.gov.pl/bip/_files_/bip/bip_projekty_aktow_prawnych/oc/2009/ustawa_gry_13.11/projekt___nowelizacji_z__13_11_09_-_2__2_.pdf.

could be used to make financial transactions without the consent of the trustee of the funds; (iv) content being illegal advertising or promotion or enabling the organization of gambling without any authorization granted or participation in these games. Pursuant to this regulation, access providers were to be obliged to immediately block access to websites or services recorded in the Register of Prohibited Websites and Services. The amendments, however, never came into force.

- In 2013, the Parliamentary Committee on Administration and Digitization presented a resolution obliging the Ministry of Administration and Digitization to "prepare **the technical and legal solutions that guarantee parents the right of access to the Internet free from pornography**".[33] According to the resolution, "ISPs should [free] to provide tools to block transmission of pornographic materials". The Members of Parliament also suggested that providers should provide users an alternative offer - access to the Internet without pornography. The resolution generated, however, a lot of doubts. In particular, it was not clear if tools that were to be implemented by the Internet service providers should have relied on filtering and in what circumstances. One interpretation led to the conclusion that it should be understood only as an incentive to create family filters (operating at the level of the home network). However, in accordance with a more far-reaching and commonly-held interpretation, the resolution could have been the basis for the introduction of mechanisms to censor Web content by Internet service providers.
- In December, 2014, the Deputy Minister of Finance made a statement that the Ministry of Finance considered the introduction of mechanisms enabling the **blocking of illegal gambling sites** as an effective way to organize the market and limit unfair competition. According to the Minister's statement this concept will not, however, be advanced during the current Parliament's term of office.[34]

The solutions imposing a duty to block and filter content by access providers **are criticized by legal doctrine and associations of ISPs**. It is said that the obligations to block the content and to develop effective filters would be contradictory to the provisions of applicable law concerning the liability of ISPs including access providers. Effective filtering and blocking of Internet illegal content would require permanent monitoring of all data transmitted by them (in order to eliminate the category of illegal content defined in the regulations). Such a general obligation is, however, in contradiction with both the provisions of domestic law and the E-Commerce Directive (in this regard see section 4 below).

Moreover, it is stressed that the imposition of such an obligation could cause a breach of the **principle of network neutrality** understood as "the principle that all electronic communications passing through the network are treated equally, in particular, be treated equally regardless of their content, applications, services, devices and the address of the sender and recipient address".

These kind of regulations can also lead to **violations of freedom of expression**. In this regard, it is said that the introduction of filters can have a negative impact on the availability of legal content on the Internet - filters can lead to restricting access to content on the Internet, and consequently threaten freedom of expression and the free access to content on the Internet.

2.1.2. Blocking/filtering on a case by case basis

---

33 The draft of resolution calling on the Minister of Administration and Digitization to ensure the parents the rights to the Internet without pornography, Warsaw, 29th July, 2013, available at: http://orka.sejm.gov.pl/Druki7ka.nsf/0/107F92BAF489D5EAC1257BD500319B54/%24File/1664.pdf.

34 See e.g.,. the press report available at: http://wyborcza.biz/biznes/1,100896,17063446,Polska_zablokuje_nielegalnych_e_bukmacherow_juz_w.html#ixzz3KqL73VLC.

As already mentioned, under Polish regulations, **a court or other competent authority may, in the decision passed within the relevant proceedings, order the ISP to make the access to the content impossible** (by blocking or removing it). With regard to the access providers the rules provided in Art. 12 of the Act on Providing Services by Electronic Means apply, since this regulation concerns the services rendered by both access providers and network providers.[35] According to Art. 12 of the Act the liability for the conveyed data shall not be borne by the one who, while transmitting data, (i) is not an initiator of the transmission, (ii) does not select the recipient of data, and (iii) does not delete or modify the data being subject to transmission. Thus, generally **the courts or other authorities are able to order an access provider to block the content only if this entity can be effectively sued under this regulation (as perpetrator or aiding person)**. The exception to this rule is, however, provided under criminal procedure (in this regard see section 3 below - the forfeiture of items).

It should be however mentioned that the decision on blocking the content **should be related solely to the illegal content**. The problem may arise, however, when on the website there are both infringing materials and legal content. Given that the measures applied by courts and public authorities cannot deprive access to legal content (in particular in light of the freedom of expression) blocking, in these circumstances, access to the Internet platform or to the entire website would likely be unfounded.

2.1.3. Self-regulations and soft law

It is also underlined in Polish legal doctrine that instead of implementing the legal provisions relating to blocking and filtering obligations, the legislator should take into account the **instruments of self-regulation and co-regulation**. Self-regulation instruments are said to be able to play an important role in delivering a high level of Internet user protection. It is believed that measures aimed at preventing illegal content on the Internet (such as for example child pornography or content concerning totalitarian regimes) are more effective if they are taken with the active support of the service providers themselves. In Poland there are some self-regulations aimed at counteracting the existence of illegal content on the Internet that constitute a type of voluntary initiative which enables economic operators, social partners, non-governmental organisations or associations to adopt common guidelines.

The protection against illegal content being achieved by the promotion of self-regulation can be treated as **an introduction of soft law to the domestic legal system**. These regulations are not enforced by the proceedings before the public courts but by members of the same community, whose proceedings are governed by the internal code. As an example of such a self-regulation instrument, one can look at the initiative worked out by the Interactive Advertising Bureau Poland (IAB Polska) with the participation of the National Broadcasting Council referring to the **Code of Good Practice on the Protection of Minors in VOD services.**[36]. The document has been signed by the largest entities from the VOD sector in Poland. The Code was created to ensure effective protection of minors from detrimental content, taking into consideration technical capabilities, the level of harm in the broadcast or other transmissions to minors in specific age categories as well as the unique characteristics of on-demand audio-visual media services. The Code was formulated in such a way as to ensure effective enforcement of the regulations contained therein. According to the signed document, making on-demand media services publically available, which includes content that is unsuitable for underage viewers, may take place only and exclusively alongside the use of technical protective measures which effectively verify the viewer is of appropriate age. Proposed solutions include age verification through the use of credit card data or through payment upon first access to

---

35 W. Chomiczewski, Komentarz do art. 12 ustawy o świadczeniu usług drogą elektroniczną, Lex 2011.

36 Kodeks dobrych praktyk VOD w zakresie ochrony małoletnich. Available at http://iab.org.pl/wp-content/uploads/2014/07/iab_kdp_vod_maloletni_2014.pdf (15.08.2015).

the inappropriate content (e.g. through the use of a credit card, bank transfer, etc.). Insofar as it is technically possible, providers may also set up a so-called safe mode, which filters inappropriate content and which may be deactivated only after verifying the viewer is of appropriate age. Verification should be done through entering, for example, an alphanumeric PIN code or other equivalent solution.

2.1.4. Voluntary activities on blocking/filtering

What is more, apart from the possibilities of blocking/filtering Internet content by access providers being the telco operators, there are some solutions regarding **blocking and filtering content by the private and public entities**. Generally, Polish law does not prohibit filtering and blocking content on local networks. Therefore, private companies or public institutions can create their own internal networks for employees or customers and use some tools in order to make access to certain content impossible. Since the local networks are not available to the general public and they serve the particular purposes, it seems that blocking of the content which is not consistent with these goals can be justified. In this regard the following mechanisms can be pointed out:

- Lots of **private firms** block access to social media or online games to counteract the wasting of time with such activities by their employees.
- Blocking access to Internet content is also commonly used by **educational institutions**. According to the Polish NGO report, over 62% of libraries in Poland use internet content blocking solutions.[37]
- There have also been implemented some initiatives on the protection of students in **schools** from illegal content. In 2006, on the basis of an agreement between the Ministry of Education and the Catholic Cultural Centre, the program called Benjamin was made available (free of charge) for schools and all individuals who wished to use it for non-commercial purposes. The project was, however, criticized because of the list of words blocked by it. For example, within the counteracting drug addiction policy, all pages containing the word "drugs" were blocked. As a consequence, websites regarding anti-drug campaigns and information about points of assistance for addicted persons were also blocked.

What is more, **blocking Internet content may also take place on the demand of individuals**, if the owner of an end device (i.a. computer) has ordered and installed the appropriate filter. This should be treated as a commercial service, operating solely on the device on which it is installed. Therefore, it does not affect the availability of the content for other users. In Poland, the tools (including free of charge solutions) allowing individuals to filter inappropriate content are widely available and commonly used. It is, however, said that the use of such solutions does not arouse controversy in light of personal rights protection (especially the freedom of expression and right to access to information) and the network neutrality principle.

2.2. Take-down/removal of illegal Internet content

Since there is **no specific law on taking down illegal Internet content in Poland,** the only way to order an internet provider to take down/remove illegal internet content is, currently, by a **court or public authority decision in force.** Therefore, the ISP must be the subject of an action before the court (see, however, the exemption indicated in section 3 - the forfeiture of items) or before the public administration body.

---

[37] M. Maj & K. Szymielewicz (Fundacja Panoptykon), Perypetie informacji w Internecie. Przewodnik. Available at https://perypetie-informacji.panoptykon.org/images/perypetie-informacji.pdf (15.08.2015).

Under Polish law, there are no special regulations on the responsibility of internet service providers. Therefore, the general rules on the ground of civil, criminal and administration law apply in this regard together with the provisions of the Act on Providing Services by Electronic Means concerning the exclusion of ISPs' liability. The following regulations should be considered in this context:

- Pursuant to Art. 14 of the Act (referring to **hosting services**), the responsibility for the stored data shall not be borne by the entity, who, making the resources of a communication system available for the purpose of the data storage by service recipient, is not aware of the unlawful nature of the data or the activity related to them, or having been officially informed or having received a credible notice on the unlawful nature of the data or the activity related to them, makes the access to the data immediately impossible. The following exception is applicable to all sorts of websites, including social networking sites.[38]
- In accordance with Art. 13 of the Act (concerning **caching services**), the responsibility for the stored data shall not be borne by the entity transmitting data and providing for automated and short-term indirect storing of the data in order to make them quickly accessible on the request of another entity, whenever such entity (i) does not delete or modify the data; (ii) uses recognised and usually applied in such activity information techniques determining technical parameters of data access and their updating, (iii) does not interfere with using of information techniques, recognised and usually applied in this kind of activity for gathering information about usage of the collected data. What is more, responsibility for the stored data shall not be borne by the entity who, respecting the abovementioned conditions, immediately removes the data or makes the access to the stored data impossible as soon as he/she receives the message that the data have been removed from the initial source of transmission or the access to them has been made impossible, or **a court or any other competent authority has ordered the removal of the data or made access to them impossible**. The latter situation is rather hypothetical. From a practical point of view, suing the caching provider to obtain a judgment ordering him to remove the data is useless. Even if the court orders the caching provider to delete the data, they will remain on the source server and the access to them by network users will be still possible. Hence, it is more reasonable to direct an action against the hosting provider or content provider and thereby gain a writ of execution providing for the obligation to remove the data from the source server or prevent access to the data on the source server.[39]

2.2.1. Notice and take down procedure

Poland has not implemented **any precise "notice and take-down procedure"** dealing with the formal and procedural requirements of a notice on unlawful content to the ISP. What is more, the terms "official information", "credible notice" and "immediately" used in Art. 14 of the Act (above) have not been defined in the Act on Providing Services by Electronic Means nor in accompanying jurisprudence, resulting in much autonomy for ISPs in making their decisions. This autonomy requires ISPs to make autonomous decisions on the credibility of the information received, legality of content and due time for such content to be disabled. Thus, there is **no detailed notice and take-down procedure** in place on the formal and procedural conditions of filing a notice and its consequences.

There is also **no coherent self-regulation at the level of associations of intermediaries in this regard**, with individual service providers making their decision individually. Regardless of the statutory notice and take-down procedure, some providers have, however, developed their own standards.

This situation causes an undesired **chilling effect resulting in intermediary service providers disabling most content reported as potentially illegal in order to avoid any liability**. Accordingly, for

---

38 Appellate Court in Wroclaw Judgment dated 15 January 2010, I ACa 1202/09.

39 W. Chomiczewski, Komentarz do art. 13 ustawy o świadczeniu usług drogą elektroniczną, Lex 2011.

several years the **assumptions of amendments to the Act** have been being discussed. According to the proposals, there are plans to implement a precise notice and take-down procedure which determine, among others, the required content of credible notice and due time for ISPs' reaction.

2.2.2. Relevant Case Law

In a judgment of the Supreme Court,[40] it was held that ISPs are responsible for the violation of personal rights performed by others only when they knew that the post violated these interests and they did not immediately prevent access to the post. Therefore, **the ISP is not obliged to control the content of posts written by users on a free discussion forum website**. Taking into account the nature and purpose of services based on making available a discussion website free of charge, and considering also that there were no general rules for the management of such services and systems, the Court held that there were **no grounds to impose a general obligation on the ISP to provide tools to identify users of such a website**. The Court ruled that the anonymity of persons using the publicly available online news website, is a generally accepted principle of this type of service. It ensures freedom of expression, which is the goal of such websites. Consequently, the Court held that the ISP that provides free access to its website with a discussion forum, has no obligation to ensure the ability to identify the users who created posts on this website. This case might not be in line with the newest Grand Chamber Judgement in the case Delfi A.S. v. Estonia.[41] However, we should wait for new Polish court decisions to say how the case Delfi A.S. v. Estonia will impact on the Polish jurisprudence.

In addition, one should also mention that very recently, the Regional Court in Kraków[42] ordered an ISP to monitor platforms on a monthly basis in order to block files specified in the court ruling (which violated copyrights) as they could be uploaded again. This case is not final yet as it might still be appealed (in this regard see also section 5).

The District Court in Szczecin[43] held that the administrator of an Internet forum cannot be held responsible for comments that appeared on his website, unless it is proved that the content of posts/comments was illegal, and that the administrator had knowledge regarding such posts or comments, or has received information from a reliable source regarding such posts or comments, and did not fulfil his duty to disable access to such illegal content. All these prerequisites must be met together. The Court ruled that the administrator of the internet forum cannot arbitrarily interfere with the content published by users. The Court noted that too much interference may lead to a violation of the freedom of expression, and thus it may also be an infringement of personal interests of users. The Court has also interpreted the meaning of the "credible information" of the illegal character of the stored data as provided in the Article 14 of the Act on Providing Services by Electronic Means. For the adoption of the credibility of information, it is necessary to show that on the basis of the information received, the ISP had an objective opportunity to assess the illegality of data placed on the Internet by the customer. A different interpretation – that each request of an interested person (legal or natural) which results in the receipt of credible information of the illegal character of the stored data, would mean that, in principle, anyone whose activities fall within the online forum discussion, could remove data with reference to the violation of personal interest, and it would end any discussion. As the Court noted, such a situation would be against the principle of freedom of expression and the essence of Internet activity. The Appellate Court in Szczecin[44] dismissed the complaint in this case.

---

40 Supreme Court Judgment dated 8 July 2011, IV CSK 665/10.

41 European Court of Human Rights Judgment dated 16 June 2015, 64569/09

42 Regional Court Judgment dated 27 May 2015, IX GC 791/12.

43 District Court in Szczecin VIII Economic Division Judgment dated 5 May 2011, VIII GC 106/10.

44 Appellate Court in Szczecin Judgment dated 26 October 2011, I ACa 572/11.

The District Court in Warsaw[45] found the publisher of a popular Polish portal guilty for publishing information about the social status of a Polish businessman and his wife (being a famous Polish journalist) and their new house, which was built on a grand scale. The Court held that the content of articles undermined the prestige of the spouses as they are people commonly known, reputable and rich. The Appellate Court also found the publisher guilty. The Supreme Court[46] referred the case for further reconsideration. One of the grounds was that the Court did not rule on the relationship between the comments posted by Internet users and the provisions of Polish Act on Providing Services by Electronic Means that exclude the liability of the ISPs.

The Supreme Court in the case I CSK 128/13[47] referred to the case Delfi A.S. v. Estonia and concluded that there is room in the national legal framework for solutions limiting the freedom of expression, when the violating content is offensive and hateful, where the ISP is not providing for sufficient prevention, is deriving benefits from this content, and ensures the anonymity of authors of hate speech. It added that the service provider, who has implemented an automatic system to prevent access to the comments that contain vulgarity, will have knowledge of the illegal comments which contain vulgarity (and accordingly might be held liable for such illegal content).

3. Procedural Aspects

In Poland, there are **no specific laws on blocking, filtering or take down of illegal internet content**. The only way to order a host provider to take down/remove or to order an access provider to filter/block illegal internet content **is a decision of a court or public administration body**. Since there are no special laws on the responsibility of internet service providers, the **general rules apply.**

3.1. Criminal Procedure

The Code of Criminal Procedure[48] **allows prosecutors and courts to demand and seize objects including computer data and information systems** (together with media or devices, which were used to host this data), which could serve as evidence or in order to secure penalties regarding property, penal measure involving property or claims to redress damage. In the course of the criminal proceedings, this provision might be the legal basis for the seizure of servers which host websites with illegal content (e.g. child pornography website). As a consequence of the order of a prosecutor or a court, **the website with illegal content will be removed**. Additionally, in urgent cases (not amenable to delay) the police or other authorized agency may seize such objects. However, **all orders based on this provision might be appealed before an independent court** (a prosecutor or police order, may be appealed before the court and a court order may be appealed before the court of appeal). The party that is the addressee of such order will be notified.

Furthermore, the illegal content might be blocked/removed by a criminal court in a **judgment**. According to the Penal Code,[49] the court imposes **the forfeiture of items directly relating to an offence**. This provision might be the legal basis for removing the illegal child pornography website or content violating copyrights. The judgment which imposes the forfeiture is issued against the convicted person (a party to the proceeding). However, **under this judgment, third parties might also be obliged to block/remove the illegal content**. The judgment should always be

45 District Court in Warsaw Judgment dated 24 October 2011, IV C 1639/10.
46 Supreme Court Judgment dated 12 September 2014, I CSK 542/13.
47 Supreme Court Judgment dated 10 January 2014, I CSK 128/13.
48 Code of Criminal Procedure Section 217.
49 Penal Code Section 44.1.

announced/appropriately delivered. The judgment might be appealed. It should be mentioned that even if there is no known jurisprudence on the removal/blocking Internet content based on the provisions of forfeiture of items, it is reasonable that criminal courts should have such legal grounds (and this seems suitable for such purpose).

3.2. Civil Procedure

The Code of Civil Procedure also allows courts to render decisions requiring ISPs to block/remove the illegal content. In the course of civil proceedings, a civil court may issue an **interim measure (injunctive relief)**[50] **which obliges an ISP (which is a party in civil proceedings) to remove/block the disputable content** for a defined period (until the end of the proceedings). Please see below the example of wording, which is usually used for injunctive relief:

"*The Regional Court (…) has decided: to grant injunctive relief with respect to the claim of the Claimant, against the Defendant for the protection of personal rights by ordering that the Defendant ceases the infringement and deletes certain entries from the blog available on the website which form part of the information and communication technology resources provided by the Claimant, by ordering that the Defendant deletes the following entries from the subpage URL (…) for a period of 1 (one) year."*

The decision of a court on injunctive relief which is delivered to the ISP might be appealed (interlocutory appeal).

Additionally, **civil courts may force the ISP to remove/block the illegal content in the final judgment**. The legal basis for the court's judgment requiring the intermediary to remove the content is the substantive law (e.g. in case of infringement of personal rights, the court may order the removal of the state of violation, e.g. by destroying the false opinion or objects used to violate the personal rights; in the case of copyright, the author may request that the person who committed the infringement should perform all the actions necessary for elimination of its effects – see section 2 above). The ISP should be a party to the civil proceeding (as perpetrator or as aiding person). It should be emphasized that the court strictly specifies in the judgment the steps required to be made.[51] The judgment is announced to the defendant (ISP) and it may be appealed before the court of appeal.

3.3. Administrative Procedure

Furthermore, the public administration authority may also require the removing/blocking of the illegal content/data. **The Polish DPA** is entitled to*, ex officio* or upon a motion of a person concerned, by means of an administrative decision, **order the restoration of the proper legal state**, and in particular, *inter alia*, **to remedy the negligence**, **not to disclose personal data** or **to erase the personal data**.[52] The ISP might be only bound by the decision of the DPA if it is issued against the ISP (after the administrative proceedings based on the Code of Administrative Procedure). The ISP is notified of the obligation by the delivery of the administrative decision of the DPA. Subsequently, the ISP may file a motion for reexamination of the case to the DPA and then, if the decision is upheld, appeal before the administrative courts.

The Code of Administrative Procedure is also the basis for decisions of **the President of the Office of Competition and Consumer Protection** on pronouncing a practice as violating collective consumer interests and **ordering that the same be discontinued.** The ISP is notified by the delivery of the

---

50 Code of Civil Procedure Section 730.1.

51 Supreme Court Judgment dated 22 December 1997. II CKN 546/97.

52 Act on Personal Data Protection Section 18.

administrative decision of President of the Office of Competition and Consumer Protection. Intermediary (addressee of the decision) might appeal to the Court of Competition and Consumer Protection.
Additionally, the **Chairman of the National Broadcasting Counci**l may, acting by virtue of the National Broadcasting Council's resolution, **issue a decision ordering the media service provider to cease the practices, referred to as provision of media services, if they infringe upon the provisions of the Act**. Such decisions might be appealed to administrative courts.

If the abovementioned **decisions of courts or public administration authorities are final and binding, the addressee** (intermediary) **should perform the imposed obligations**. If such ISP does not comply with these decisions (e.g. Search Engine did not block/remove the URLs mentioned in the injunctive relief, or the social network provider did not remove the personal data according to the decision of DPA), there are appropriate instruments, which may force ISP to remove/block the content (e.g. Code of Civil Procedure,[53] or Act on Enforcement Procedure in Administration). Under these provisions, the District Court may impose a fine to the ISP for not blocking/removing the content.

3.4. Other regulations

There is also different procedure for domain names disputes, which may result in removing the whole website. **NASK** (*Naukowa i Akademicka Sieć Komputerowa* - the Research and Academic Computer Network) administers the national registry of internet names with the .pl domain. Domain name disputes are resolved under Polish law by one of the two arbitration courts and pursuant to their rules (the permanent arbitration courts operating at organizations connected with NASK by co-operation agreements on disputes resolution are the Arbitration Court at the Polish Chamber of Information Technology and Telecommunication in Warsaw and the Court of Arbitration at the Polish Chamber of Commerce in Warsaw).[54] Violation of rights (e.g. trademarks) might result in arbitration proceedings and the **Arbitration Court's award might be the basis for NASK to transfer the domain name to a rights holder.**

It is clearly crucial for the claimant whose rights have been violated by registration or maintenance of a domain name that the arbitration award be legally effective. In resolving the dispute, the arbitrator issues an award that is treated like a judgment for the purposes of the Code of Civil Procedure. This means that the award has the same legal force as a judgment by a state court and may be enforced upon issuance of an enforcement clause by the state court that would have had jurisdiction over the dispute had it not gone to arbitration. Upon issuance of the enforcement clause, the arbitration award becomes a writ of enforcement, binding on the parties as well as courts and other state bodies. The award also enjoys *res judicata* effect. [55]

It should be borne in mind that no appeal as such lies against an award issued by the Internet Domains Arbitration Court. **Judicial review of the award may be sought by filing a petition with the state court to set aside the award.** The award may be set aside only if one of the specific grounds provided in the Code of Civil Procedure is proved.[56]

---

53 Code of Civil Procedure Part 3 (Enforcement Procedure).

54 K. Wisniewska. Cybersquatting and resolving of domain name disputes in Poland. COFOLA 2011: the Conference Proceedings, 1. edition. Brno: Masaryk University, 2011. Available at: http://www.law.muni.cz/sborniky/cofola2011/files/IT/vlastnictvi/Wisniewska_Katarzyna_6038.pdf.

55 D. Kwiatkiewicz-Trzaskowska. Co do zasady. Avalable at: http://www.codozasady.pl/en/domain-disputes/

56 D. Kwiatkiewicz-Trzaskowska. *Ibidem*.

Accordingly, there is **no specific law on blocking, filtering or taking down illegal internet content; however, the abovementioned judiciary and administrative bodies have power to impel intermediaries (or other entities) to block/remove the illegal Internet content.**

4. General Monitoring of Internet

There is **no Polish legislation on general monitoring of the content of the Internet.** Article 15 of the E-Commerce Directive (prohibiting Member States from imposing a general obligation on intermediaries to monitor the information which they transmit or store) was transposed into the Art. 15 of the Polish Act on Providing Services by Electronic Means. According to this Act, the entity which provides services specified in the Art. 12 (mere conduit), Art. 13 (caching) and Art. 14 (hosting) should not be obliged to monitor the data referred to in these articles, which are transmitted, stored or made available by that entity.

Additionally, the District Court in Wroclaw in its judgment (case no. I C 988/13)[57] ruled that the lack of implementation of a control and content filtering system for profanity comments cannot prejudge the responsibility of the defendant, because **preventive censorship would lead to infringement of the right to freedom of expression**. The decision on the scope and priority of protected and conflicting rights, while accepting the obligation to adopt preventive control of information posted on a website and bonding the liability of the provider with the lack of such system, would constitute an excessive interference in the need of protection for different rights and interests, while simultaneously threatening freedom of expression. Similar phrases were also expressed by other courts (e.g. case no. I ACa 544/10, case no. II CSK 747/13, case no. IV CSK 665/10).

The review of Internet content for its compliance with legal requirements takes place, in practice, under essentially voluntary notices of right holders (possibly illegal material is typically brought to the attention of the ISP by other users rather than through active monitoring by the intermediary). However, **Art. 15 of the Act is not an obstacle for courts (and public authorities) to impose on ISPs (referred to in Art. 12, 13 and 14 of the Act) an obligation to monitor (which means in practice: removing/blocking) specific data (specific URL), which was the subject of the proceedings.**[58]

Nonetheless, there is a governmental agency, which **might be viewed as the entity responsible for monitoring the Web and for looking for any illegal content. Police, particularly the Unit For the Fight Against Cybercrime at General Police Headquarters of Poland** (*Wydział do walki z Cyberprzestępczością w Komendzie Głównej Policji*) and local units for the fight against cybercrime at other headquarters (e.g. at Warsaw Metropolitan Police Headquarter) are monitoring the Internet in this regard. It should be stressed that the role of the police units is **detecting criminal offences and preventing the commission of new online crimes**. The **Police has no power to block, filter, or take down illegal content** (it might be only done by the ISP based on a court or public administration authority's decision). The Units For the Fight Against Cybercrime monitor the Web on a daily basis (they also use some electronic systems, which automatically find keywords connected with illegal content).

Furthermore, under the Act on Police (Art. 19), the Regional Court (*Sąd Okręgowy*) may issue a decision, which entitles the police to conduct "**operating surveillance**" (*kontrola operacyjna).* It authorizes police to invigilate all telecommunication data, which is transferred by a specified user. Accordingly, on the basis of a court's decision, the police may receive access to the mailbox of a user of the ISP (**monitor incoming and outgoing e-mails**). The criminal proceedings conducted by the

---

57 District Court Judgment dated 26 September 2014, I C 988/13.

58 W. Chomiczewski, Komentarz do art. 15 ustawy o świadczeniu usług drogą elektroniczną, Lex 2011.

police is supervised by a prosecutor. Additionally, some other law enforcement authorities (e.g. Internal Security Office) are entitled to receive such access based on a court's decision. Additionally, there is a hotline that has been functioning within the framework of NASK: the Dyżurnet.pl. It responds to anonymous reports received from Internet users about potentially illegal material, such as pornographic content involving a minor. The hotline informs police about the illegal content.

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

5.1. Assessment of the legal provisions on which blocking, filtering and take down measures are based

According to the art. 10 of the Convention, the **restriction of the freedom of expression is only possible if it is "prescribed by law", "necessary in a democratic society" and "in the interests of legitimate goals".** Similarly the Constitution of the Republic of Poland provides for the conditions for limitations of the constitutional rights and freedoms (e.g. freedom of expression – art. 54 of the Constitution). Any limitation may be imposed only by statute, and only when necessary in a democratic state for the protection of legitimate goals (art. 31 para. 3 of the Constitution).

First of all, the limitation of the freedom of expression **might only be introduced by Statute**. It means that it might only be imposed by written law, enacted by the parliament. The regulations described in the section 2 above (civil law, criminal law, copyright law, trademark law, personal data protection law etc.) are laws enacted by the parliament and therefore fulfill this condition.

The aforementioned regulations further meet the requirements of foreseeability, accessibility, clarity and precision as developed by the European Court of Human Rights. The procedural law (e.g. Code of Civil Procedure, Code of Criminal Procedure, as mentioned in the section 3) and substantive law (as mentioned in the section 2) indicate **the scope of discretion and precision of a court** (or a public authority) in taking a decision on removal/blocking of the content. In every case a court (or public administration body) will thoroughly evaluate circumstances for blocking/removal. In most cases a blocking decision will be narrowed and target specific links.[59] Furthermore, the rule of good legislation, which results from the Polish Constitution, requires the establishment of a law which is **clear** for citizens. The law, which might be a basis for blocking and removing content, is sufficiently precise to enable citizens to reasonably **foresee the consequences** which a given action may entail. Additionally, **the accessibility to the law** condition is fulfilled as the relevant legal acts are published in the Journal of Law (available to the public). Accordingly, the law provides 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.

Secondly, the limitation of the freedom of expression **must be necessary for a democratic society** (the **proportionality** principle).[60] The bases for blocking and removing content from the Internet are proportionate. The implementation of the E- Commerce Directive ensures that ISPs are not obliged to monitor the content on their platforms. Additionally, ISPs are not held liable for the illegal content hosted on their platforms if they block the content after they receive a notification about the unlawful nature of the content (please see the section 2 above). Furthermore, another instrument is a general clause in the Civil Code, which protects from **abuse of rights** (e.g. using some rights not to protect own interests but only in order to remove someone's content). Under art. 5 of the Civil Code:

---

59 Exceptionally it might be also broader as in the case Chomikuj, no. IX GC 791/12, please see section 5.3. below.

60 M. Macovei, Freedom of expression: A guide to the implementation of Article 10 of the European Convention on Human Rights, Council of Europe 2001, 2004, p. 35.

"one cannot exercise one's right in a manner contradictory to its social and economic purpose or the principles of community life. Acting or refraining from acting by an entitled person is not deemed to be an exercise of that right and is not protected". This general clause should be viewed as **an instrument to ensure proportionality between rights** (as it guards against abuse). In addition, if someone's right was infringed by the blocking of content on the Internet (based on a notification of another user), such person can also bring an action to the court in order to advocate its right. Accordingly, these and other measures ensure that the restriction put on freedom of expression through decisions (orders) to block illegal content remains proportionate.

Finally, limitations of freedom of expression have to **pursue a legitimate goal.** The European Convention on Human Rights (article 10 paragraph 2) specifies all legitimate goals: "interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary". Similar conditions are prescribed by the Polish Constitution (art. 31 para 3). **Any Polish legal acts allowing for blocking/removing content aim at protecting the rights or reputation of others**. They all protect infringements of another person's right (e.g. personal rights, intellectual property rights, and personal data) and thus pursue a legitimate goal.

Taking into account the above, the substantive regulations, which might be bases for removal of the Internet content fulfill the necessity and proportionality test of the restrictions to the Freedom of Expression (as required by the European Convention on Human Rights and the Constitution of the Republic of Poland).

One should however mention that, with respect to take down procedures, the **lack of precise legal implementation of the notice and take-down procedure** results in an undesired **chilling effect for intermediary service providers who are tempted, in order to avoid any risk of liability, to disable most content reported as potentially illegal**.

5.1. Assessment of the relevant domestic case-law

Polish jurisprudence appears to be in line with the pertinent case-law of the European Court of Human Rights (ECHR). First of all, while the **Supreme Court** (in the case I CSK 128/13)[61] **was evaluating the conditions of limitation of liability of ISPs, it referred to the case Delfi A.S. v. Estonia**[62]. In this case, the ECHR held an ISP liable for the appearance of abusive comments. The Supreme Court also concluded that **there is room in the national legal framework for solutions limiting the freedom of expression, when the violating content is offensive and hateful, the ISP is not providing for sufficient prevention, is deriving benefits from this content, and ensures the anonymity of authors of hate speech**.

Nonetheless, the abovementioned case is rather an exception, as usually Polish courts state that **there is no obligation of ISP to monitor the content** (case no. I ACa 544/10[63], case no. II CSK 747/13[64], case no. IV CSK 665/10[65]). All these cases confirmed that ISPs might only be held liable for third-party content if they had knowledge of illegal activities. It should be noted that the cases no. II CSK 747/13 and no. IV CSK 665/10 concerned non-commercial platforms, so they were different to the case I CSK 128/13 and the case Delfi A.S. v. Estonia. In the case I CSK 128/13, the court underlined

61 Supreme Court Judgment dated 10 January 2014, I CSK 128/13.

62 European Court of Human Rights Judgment dated 10 October 2013, 64569/09

63 Appellate Court Judgment dated 18 January 2014, I ACa 544/10.

64 Supreme Court Judgment dated 14 January 2015, II CSK 747/13.

65 Supreme Court Judgment dated 8 July 2011, IV CSK 665/10.

that an ISP derives benefits from this content, so long as it does not provide for sufficient prevention from hateful comments, there is room in the national legal framework for solutions to limit the freedom of expression. **Nonetheless, most Polish jurisprudence confirms that there is no obligation on an ISP to monitor content.** Obviously, we cannot exclude that the newest Grand Chamber Judgment in the case Delfi A.S. v. Estonia[66] will impact on the Polish jurisprudence in the future. Any change in the jurisprudence approach may cause the **chilling effect** resulting in intermediary service providers disabling most content reported as potentially illegal in order to avoid any liability.

It should be also noted that recently, the Regional Court in Kraków (in the case of famous hosting platform: Chomikuj, no. IX GC 791/12[67]) made an exception in the abovementioned line of case-law. The court ordered the ISP to **monitor platforms on a monthly basis** in order to block files specified in the court ruling (which violated copyrights) as they could be uploaded again. Such a case is new in Poland, and not final yet as it might still be appealed.

There is also other line of case law in line with the case law of the ECHR in terms of freedom of expression. **The Supreme Court (in the case no. I CSK 743/10)[68] referred to the Times Newspapers Ltd. v. United Kingdom[69]** and agreed that libelling by the continued publication on the Internet (online article) was a violation of personal rights, entitling the plaintiff to bring an action to a court independently of the previous lawsuits for the same article published in the paper edition of the newspaper. Furthermore, the domestic courts' decisions in the case of **Smolczewski i Węgrzynowski v. Poland** (which lead to a case before the ECHR[70]) stated that it was not for courts to order that the article is expunged as if it had never existed (as it is in line with Times Newspapers Ltd case). The ECHR accepted that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publications which have in the past been found, by final judicial decisions, to amount to unjustified attacks on individual reputations (as the legitimate interest of the public to access to the public Internet archives of the press is protected under Article 10 of the Convention).

Accordingly, the domestic case law is generally in line with the case law of the European Court of Human Rights.

Xawery Konarsky
Attorney-at-Law
15 October 2015

66 European Court of Human Rights Judgment dated 16 June 2015, 64569/09
67 Regional Court Judgment dated 27 May 2015, IX GC 791/12.
68 Supreme Court Judgment dated 28 September 2011, I CSK 743/10.
69 European Court of Human Rights Judgment dated 10 March 2009, 3002/03 and 23676/03.
70 European Court of Human Rights Judgment dated 16 July 2013, 33846/07